On the ℓ-adic representations of the Galois groups of number fields

By

SONG Li-Min

A thesis

Submitted to

the Graduate School of

The Chinese University of Hong Kong

(Division of Mathematics)

In Partial Fulfillment of the Requirement for

the Degree of Master of Philosophy

May, 1987

Acknowldgement :

I would like to thank Dr. K.F. Lai for the suggession of the topic and the advices, and that he showed me the background knowledge of algebraic geometry, particularly those mentioned in the INTRODUCTION.

Abstract

This thesis concerns with the ℓ-adic representations of the Galois groups of number fields obtained from varieties. The study of these ℓ-adic representations may be one way to study the (arithmetic of the) varieties themselves. The general theory of ℓ-adic representations of number fields ad hoc due to Serre is also treated here.

Our emphasis is on the determination of the images of the ℓ-adic representations, but mainly concentrating on the simplest case, namely, that about elliptic and modular curves.

Chapter I deals with the theory of Abelian ℓ-adic representations according to Serre. Its generalization to the λ-adic case is also treated (§10). There is another equivalent description of these ℓ-adic representations via local algebraicity (§ 8) which is convenient for us to gain knowledge from algebraic geometry. There is a complete description of the locally algebraic semi-simple rational Abelian ℓ-adic representations of number fields (§5).

Chapter II is about the ℓ-adic representations attached to elliptic curves. This is the best known result. The problem, separated into two cases: with or withoout complex multiplication, is completely solved (§ 7). Some

generalizations, particularly the case of Abelian varieties with complex multiplication (§13) and a case of Abelian varieties with real multiplication (§12), are also mentioned.

In chapter III we consider the modular curves, but we mainly consider the properties of the ℓ-adic representation of Deligne-Serre as some "axiomatic" data (this is in fact what we have done in this whole thesis). The Lie algebras of the images of the representatons are determined (§9, §10). But in group level the problem comes to be a little bit complicated because of the "extra twists". In fact we can only determine the images of a particular subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (§11) in general. The mod ℓ theory of modular forms for the simplest case $SL(2,\mathbb{Z})$ is presented in §2 which is essential as a tool for the consideration of the reduction modulo ℓ behaviour of the representations and thus for the determination of the Lie groups G_ℓ. The general properties of the representations (§ 5) are closedly related to L-functions.

Chapter IV is a collection of some elementary facts of the group theory about $GL(2)$ and about Lie algebras. They apply in most cases to our consideraton.

Table of Content

Part 0 Introduction 1

1. 7

2. Notations. 7

Part I ℓ-adic Representations 9

1. Definition. 9

2. Basic questions. 10

2.1. A consequence of the Cebotarev Density Theorem ...10

2.2. Unramifiedness. 12

2.3. Rationality. 12

2.4. Compatibility 13

2.5. Compatibility of a system of ℓ-adic representations 13

2.6. Semi-simplicity; semi-simplification. 14

2.7. Abelianness. 15

2.8. Representation with values in an algebraic group..16

3. Examples 16

3.1. Elliptic curve over purely transcendental field ..19

4. Some facts in classfield theory; reciprocity. 20

4.0. Some notations. 20

4.1. Decomposition subgroup, inertia subgrou and the Frobenius automorphism. 20

4.2. Global reciprocity map. 22

4.3. Local reciprocity map. 22

4.4. Relation between local and global 22

5. The representation attached to a Serre's torus. 23
5.1. The construction of the algebraic groups 24
T_m and S_m
5.2. The canonical representation ξ_ℓ 25
5.3. The property of ξ_ℓ 26
5.4. The representation associated to a 27
linear representation of S_m.
6. Characters of T_m. 29
6.1. Characters related to that of T. 29
6.2. Some formulas. 29
6.3. Examples: the case $K = \mathbb{Q}$, $S = \phi$. 30
6.4. Another formula. 32
7. Structure of $X(T_m)$. 34
7.1. The Frobenius. 35
7.2. The Frobenius (cont'd) 36
8. Local algebraicity. 37
8.1. Local case 37
8.2. Global case. 39
8.3. An example. 40
8.4. Module of local algebraicity; the equivalence 41
of locally algebraic representation and that
associated to Serre's torus; the theorem of
Serre and Lang.
8.5. Tate's theorem. 44
9. The relation with the reduction. 45
9.1. A lifting theorem of Serre. 45
9.2. Tame inertia: the exact image. 48
9.3. Characters of $\mathbb{Q}$ unramified outside p. 50
10. λ-adic representations. 50
10.1 The definition. 51

10.2 Basic questions. 52
10.3 The representation attached to a Serre's torus. ..52
10.4 Local algebraicity. 53
10.5 Some related results. 53

Part II The ℓ-adic representations attached to elliptic curves. 55
1. Definition and basic facts. 55
1.1. Elliptic curves. 55
1.2. Division points of elliptic curves. 56
1.3. The ℓ-adic representations attached to elliptic curves. ..57
1.4. Complex multiplication. 60
1.5. Good reduction. 61
1.6. Types. 63
1.7. Remark on CM. 65
2. An overview. 65
2.0. General consideration. 65
2.1. The Lie algebras. 67
2.2. Isogenous theorem. 68
2.3. The Lie groups G_ℓ. 68
2.4. Generalizations 69
3. Local case. 69
3.0. Notations. 69
3.1. Tate's curves. 69
3.2. Good reduction. 72
3.3. Good reduction: the crucial case $\ell = p(v)$. 73
4. Global case. 75
4.1. The CM case. 76
4.2. non CM case. 77

4.3. A remark. 80
5. Isogeny and Tate's module. 80
5.1. Local case 80
5.2. Global case 83
6. Density theorem 84
7. Variation of ℓ. 86
7.1. The non CM case. 87
7.2. CM case. 90
8. The proof of thm.22: non CM case 92
8.1. Preliminary results. 93
9. Elliptic curves over $\mathbb{Q}$ 95
9.1. Exceptional primes. 96
9.2. The image of ϕ_∞. 98
10. Product of two elliptic curves. 99
10.1. Notations. 99
10.2. The representation Φ_∞. 99
10.3. The proof of thm.29. 101
10.4. A remark. 103
11. Abelian varieties with real multiplication. 103
11.1. A discussion on the Lie algebras. 105
11.2. Equality between the Lie algebras. 108
11.3. The Lie groups. 109
12. A related result of Ohta. 110
13. Abelian varieties with CM. 111

Part III ℓ-adic representations attached to modular forms 114
1. Modular forms. 114
1.1. Congruence subgroups. 114
1.2. Forms with nebentypus. 115
1.3. Hecke operators, eigenforms and Euler product. ..118

1.4. Functional equation and Petersson conjecture. ..120
2. The mod ℓ theory. 121
2.1. Forms and Fourier expansion. 122
2.2. Scalar extension and reduction. 122
2.3. The q-expansion principle of Katz 123
2.4. The stucture theorem of Swinnerton-Dyer 123
2.5. Filtration. 124
2.6. Remark. 125
3. Data: the ℓ-adic representation attached to a cusp form 126
3.1. The representation. 126
3.2. A decmposition. 126
3.3. Remark. 127
3.4. Frobenius at infinity. 127
3.5. An illustation of the content. 128
4. A review of the simplest case: eigenforms for $SL(2,\mathbb{Z})$ 128
4.1. The representation and the problems. 128
4.2. Openness problem (1). 129
4.3. Exceptional primes. 130
4.4. Forms with arbitrary coefficients. 131
4.4. Remark: the case of finite product. 134
5. Basic properties of the representations. 134
6. Complex multiplication. 139
6.1. The definition. 141
7. Modular forms with complex multiplication. 142
7.1. Concrete construction. 143
7.2. Complete description. 145
8. The case k=1. 148
9. The CM case. 149
10. Forms without complex multiplication. 150

10.1. The case without extra twists. 150

10.2. Extra twists. 153

10.3. Twisting group. 154

10.4. Twisting operators. 155

10.5. The Lie algebra. 155

11. The image of $\tilde{\rho_\Omega}$. 157

Part IV Appendix: Group theory. 167

Refernces. 175

Part 0 Introduction

An ℓ-adic representation of a group is firstly a homomorphism into the general linear group with coefficients in an ℓ-adic number field. There seems to be essentially one way to construct arithmetically interesting ℓ-adic representations of Galois groups, namely, by considering the action of Galois groups on the ℓ-adic cohomology of an algebraic variety. There are two types of varieties on which we have rich information: Abelian varieties and modular varieties.

In the case of Abelian varieties, the étale cohomology is the Tate module $T_\ell(X)$ of ℓ-division points of the Abelian variety X. It was conjectured by Tate and proved by Faltings that an Abelian variety is determined upto isogeney by its Tate module. When X is an Abelian variety over a number field K such that (1) $(\mathrm{End}_K X)\otimes \mathbf{Q} = E$ is a totally real number field of degree $d=\dim X$ over $\mathbf{Q}$; (2) All endomorphisms of X are defined over K; and (3) X does not everywhere have potential good reduction, then Ribet ([2] thm 5.5.2) proves that the image of the Galois group in the mod ℓ reduction of the Tate module is

$$\{ u \in GL(2, O_E/\ell O_E) : \det(u) \in \mathbb{F}_\ell^\times \}$$

for almost all primes ℓ, where O_E is the ring of integers of E. On the other hand when the Abelian variety has complex multiplication by a subfield of the field of definition, (Serre & Tate [1] thm.5, corol.2) the ℓ-adic representation is Abelian. Among the Abelian representations we have the locally algebraic ones; they are given by algebraic representations of the Serre groups S_m (Serre [6] III §2.3.).

In the case of modular variety, a rational vector space V is constructed such that the complexification $V_{\mathbb{C}}$ is a space of automorphic forms and $V_\ell = V \otimes \mathbb{Q}_\ell$ is the cohomology of the modular variety with coefficients in an ℓ-adic sheaf; a "rational" automorphic form $\phi \in V_\ell$ then delineates an ℓ-adic representation $V_\ell(\phi)$ which is isomorphic to the ℓ-adic representation associated by the Langlands correspondence to ϕ. We are less successful in the modular case than in the case of Abelian varieties.

For curves these two cases are respectively: elliptic curves and modular curves $X_o(N)$. Here the standard problem of the ℓ-adic representation, viz., the determination of the image G_ℓ and its Lie algebra $\mathcal{G}_\ell$ of the given representation, is solved. This is the central topic of this paper.

When an elliptic curve E has complex multiplication by an imaginary quadratic extension F over $\mathbb{Q}$, the Lie algebra $\mathcal{G}_\ell$ is equal to the Cartan subalgebra of $gl(2,\mathbb{Q}_\ell)$ defined by $F \otimes \mathbb{Q}_\ell$ (Serre [2] §3.3 thm 5). If R is the

ring of integers of F then $G_\ell = R \otimes \mathbb{Z}_\ell$ for almost all ℓ (Serre [8] thm.5). When E is an elliptic curve defined over a number field K such that E does not have complex multiplication over $\bar{K}$ then for almost all ℓ we have $G_\ell = GL(2,\mathbb{Z}_\ell)$ (Serre [8] §4.2 thm.2). We shall discuss these results in chapter II.

Let us turn to the modular curves. Given two positive integers k, N. Let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ be a Dirichlet character mod N such that $\varepsilon(-1) = (-1)^k$. Let $\Gamma_0(N)$ be the subgroup of $SL(2,\mathbb{Z})$ consisting of those elements

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad c \equiv 0 \pmod{N}$$

Let f be a modular form of type (k, ε) on $\Gamma_0(N)$, in particular this means that

$$f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z) \qquad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

Assume moreover that f is an eigenform of the Hecke operators T_p with eigenvalues a_p ($p \nmid N$). Let E be a finite extension of $\mathbf{Q}$ containing the a_p and $\varepsilon(p)$. For each prime ℓ, write $E_\ell = E \otimes \mathbf{Q}_\ell$.

Theorem. There exists a continuous representation

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbb{Q}) \longrightarrow GL(2,E_\ell)$$

which is unramified outside ℓN and is such that for each $p \nmid \ell N$ we have

$$\mathrm{Tr}(\rho_\ell(F(p))) = a_p, \quad \det(\rho_\ell(F(p))) = \varepsilon(p) \cdot p^{k-1}$$

where $F(p)$ is the arithmetic Frobenius for p.

This theorem is proved in Deligne-Serre [1] for $k = 1$, basing on the same theorem for $k>1$ which is stated as Theoreme 6.1 in Deligne-Serre [1]. As pointed out in the remarque 6.2 of that paper, a special case of the theorem, for $k\geq 2$ and f a cusp form for $SL(2,\mathbb{Z})$, is proved in Deligne [1]; and "Le cas general n'est pas beaucoup plus difficile".

In Deligne [1] 3 he has shown that there is a universal elliptic curve $f : E \longrightarrow M$. Write $\widetilde{H}^1$ for the image in H^1 of the cohomology with compact support, and ${}_1^kW$ for the $\mathbb{Q}$-vector space $\widetilde{H}^1(M_1^{an}, \mathrm{Sym}^k(R^1 f_{1*}(\underline{\mathbb{Q}})))$ (Deligne [1] Definition 3.9) and S_{k+2} for the space of cusp forms of weight $k+2$ for $SL(2,\mathbb{Z})$. Then we have the Shimura isomorphism

$$ {}_1^kW \otimes \mathbb{C} = S_{k+2} \oplus \overline{S_{k+2}} $$

(loc. cit. Theoreme 2.10 and p.158) and by comparison theorem

$$ {}_1^kW \otimes \mathbb{Q}_\ell = \widetilde{H}^1(M_1 \otimes \overline{\mathbb{Q}}, \mathrm{Sym}^k(R^1 f_{1*}(\overline{\mathbb{Q}}_\ell))) $$

(loc. cit. (3.10) on p.154). The Hecke operators T_p act on ${}_1^kW$ (loc. cit. top of p.156) and the action of T_p on ${}_1^kW \otimes \mathbb{Q}_\ell$ is induced by its action on ${}_1^kW$ and is compatible with the decomposition of ${}_1^kW \otimes \mathbb{C}$ into sum of S_{k+2} and $\overline{S_{k+2}}$ (loc. cit. p.171). In this set-up, given a cuspital eigenform f in S_{k+2}, we can pick up the corresponding eigenforms of the ℓ-adic cohomology group ${}_1^kW \otimes \mathbb{Q}_\ell$. This is the special case of the above theorem.

In Chapter III we shall return to the question of the determination of the image $G_\ell = \rho_\ell(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ and the Lie algebra $\mathfrak{g}_\ell = \mathrm{Lie}(G_\ell)$ of the ℓ-adic representation given by the above theorem. It is sufficient to consider f to be a cuspital new form with eigenvalues a_p under action. Again there are two cases.

Case I. Suppose that there is a quadratic Dirichlet character $\phi : (\mathbb{Z}/D\mathbb{Z}) \longrightarrow \mathbb{C}^\times$ such that $\phi(p)a_p = a_p$ for $p \nmid DN$ and let F be the quadratic extension corresponding to the kernel of ϕ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. (F is imaginary; cf. Ribet [3] last paragraph of p.41). Then we say that f has complex multipliction by F. In this case $\rho_\ell(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is Abelian (Ribet [3] Prop.4.4) and $\mathfrak{g}_\ell = F \otimes \mathbb{Q}_\ell$ (Ribet [3] p.43 l.13).

Case II. In case that f does not have complex multiplication, write the Fourier expansion of f as

$$f = \sum_{n=1}^{\infty} a_n q^n$$

Let Γ be the set of embeddings σ into $\overline{\mathbb{Q}}$ of the field E (as given in the Deligne-Serre theorem) for which there exists a Dirichlet charcter χ_σ such that $\sigma(a_p) = \chi_\sigma(p)a_p$ for almost all p. Let $F = E^\Gamma$ be the fixed field of Γ. Then there is a 2-cocycle $c(\sigma, \delta)$ on Γ with values in $E^\times$ defined by a Jacobi sum using χ_σ and χ_δ. This cocycle defines a central simple algebra X over F. The class of X in the Brauer Group of F is represented by a quaternion al-

gebra D over F. Let $\mathcal{A}$ be the space consisting of those x in D with reduced trace Trd(x) in $\mathbb{Q}$. Momose ([1] Theorem (4.1)) proves

$$\mathcal{G}_\ell = \mathcal{A} \otimes \mathbb{Q}_\ell .$$

Each χ_σ can be considered as a character of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Let H be the intersection of $\ker\chi_\sigma$ for $\sigma \in \Gamma$. Then there is an X-module V such that the representation ρ_ℓ is realized on $V_\ell = V \otimes \mathbf{Q}_\ell$ and the actions of X and of H on V_ℓ commutes. Since the centralizer of X is D, the restriction of ρ_ℓ to H is realized as

$$\rho_\ell : H \longrightarrow (D \otimes \mathbb{Q}_\ell)^\times$$

Let $A_\ell = \{ x \in GL(2, O_F \otimes \mathbb{Z}_\ell) : \det(x) \in (\mathbb{Z}_\ell^\times)^{k-1} \}$. Then Ribet ([4] theorem 3.1) proves that for almost all ℓ,

$$\rho_\ell(H) = A_\ell .$$

1. We arrange the material as follows. The main content will be about the results for curves. On the other hand, we mention general results when possible. Not all proofs are given in full detail.

Within a chapter, different sections are devoted to distinct topics. Assumptions will remain in force the same in the whole section without further mention. We adopt the following convention: Sections and subsections are named with titles. "Proposition"s are facts, "Theorem"s are main results, and main techniques are indicated by "lemma"s. (However they are more or less mixed.)

We will quote results from Part IV by an extra letter "A": "thm.3A" means thm.3 of Part IV.

2. Notations.

Σ: the set of all finite places of a number field;

v, w : places;

p(v), ℓ(v) : residue characteristic or a rational prime that is divisible by v;

D(v), I(v) : the decomposition and inertia subgroup, resp.;

F(v) : Frobenius (class) of a number field at a place v;

ρ_ℓ, π_ℓ, ρ_λ, π_λ: ℓ-adic, resp. λ-adic representations; $F(v)\rho_\ell = \rho_\ell(F(v))$ for a representation ρ_ℓ;

χ_ℓ: cyclotomic character;

μ : the group of roots of unity (in a field);

μ_n : the subgroup of μ of order n (or ℓ^n if a prime ℓ is under discussion and no confusion appears;

G : Galois group $\mathrm{Gal}(\overline{K}/K)$ when K is fixed under discussion;

G_ℓ : image $\rho_\ell(G)$;

$G_\ell^{\sim}$: the image of G_ℓ under reduction modulo ℓ;

$\mathbb{F}_q$: the field of q elements where $q = p^n$;

$T_\ell(E)$ resp. $T_\ell(X)$: the Tate module attached to an elliptic curve E resp. an Abelian variety X;
$V_\ell(E) = T_\ell(E)\otimes\mathbb{Q}_\ell$; $V_\ell(X) = T_\ell(X)\otimes\mathbb{Q}_\ell$;

$T_\ell(\mu)$: cyclotomic module; $V_\ell(\mu) = T_\ell(\mu)\otimes\mathbb{Q}_\ell$;

$M_\ell = M\otimes\mathbb{Z}_\ell$ for a $\mathbb{Z}$-module M; it is the completion at ℓ ; $V_\ell = V\otimes\mathbb{Q}_\ell$ for a $\mathbb{Q}$-vector space V; it is the completion at ℓ;

$R^\times$: the group of units of a ring R;

$G_m = GL(1)$;

$T_{K/\mathbb{Q}}$: the torus obtained from G_m by restriction of scalar from K to $\mathbb{Q}$ where K is a number field.

Part I. ℓ-adic representations.

1. Definition.

Our main reference is Serre [6] (cited MG in this chapter, after Serre [8]).

Let K be a field; we shall denote by $\overline{K}$, K_s and K^{ab} the algebraic closure, separable closure and maximal Abelian extension of K, respectively. $Gal(L/K)$ denotes the Galois group of all automorphisms of L over K for any Galois extension L/K, endowed with Krull topology. Let ℓ be a prime number. An ℓ-adic representation of K is a continuous homomorphism

$$(1) \qquad \pi_\ell : Gal(K_s/K) \longrightarrow Aut(V),$$

where V is a finite dimensional vector space over the field $\mathbb{Q}_\ell$ of ℓ-adic numbers. For simplicity $Gal(K_s/K)$ will always be abbreviated as G only, and $Gal(K^{ab}/K)$ as G^{ab}. The image $\pi_\ell(G)$ is denoted by G_ℓ. G_ℓ is an ℓ-adic Lie group, being a closed subgroup of $Aut(V)$. Let $\mathfrak{g}_\ell$ denote its Lie algebra. (We identify $Gal(K_s/K)$ with $Gal(\overline{K}/K)$.)

2. Basic questions. Reference: MG I.

Our main interest is the ℓ-adic representations of number fields. We list some basic questions which are what we would ask when an ℓ-adic representation is given. They are the properties enjoyed in a quite natural way by the representations obtained from an variety. In this section, we assume that K is a number field which is fixed under discussion and representations are ℓ-adic representations of K. Σ is the set of all (finite) places of K. (cf. also, §7. below. For the glossary of number theory, see §4.)

2.1. A Consequence of the Cebotarev Density Theorem.

First we state a fact which gives some insight of what is to follow, and is used frequently. This is a consequence of the Cebotarev Density Theorem.

Lemma 1. (corol.2, (b), MG I §2.2) Assume that L/K is a Galois extension of number fields which is unramified outside a finite set of places. Then the set of Frobenii of unramified places is dense in $\mathrm{Gal}(L/K)$. (Note if $[L:K]$ is finite, that set is the whole $\mathrm{Gal}(L/K)$.)

2.1.1 Remark Since (cf. below) the representations we will consider (mostly come from the ℓ-adic representations

of varieties) are always unramified outside a finite set of places, i.e., they factor through extensions satisfying the condition in the above lemma, this is enough for our application, even though the representations are about $\mathrm{Gal}(\bar{K}/K)$.

2.1.2 Remark Cebotarev's Density Theorem (cf. MG I).

Let K and $\sum$ be as above and P a subset of $\sum$. Let

$$a_n(P) = \#\{ v \in P : Nv < n \}$$

where # means the cardinal number of a finite set and Nv the norm of v. Then the density of P is defined to be

$$\lim_{n\to\infty} a_n(P)/a_n(\sum)$$

if it exists. Now the Cebotarev Density Theorem states

Theorem (thm., §2.2, MG I) If L/K is a finite Galois extension of number fields, $X \subseteq \mathrm{Gal}(L/K)$ stable under conjugation, write

$$P_X = \{ v : v \text{ unramified in } L \text{ and } F(v) \subseteq X \}$$

then P_X has density $\#X/\#\mathrm{Gal}(L/K)$.

J. Tate has given a proof using the properties of L-functions. (see MG I Appendix)

2.2. Unramifiedness.

Assume an ℓ-adic representation π_ℓ of K is given in the sequal.

Let $v \in \sum$, w be a place of $\bar{K}$ extending v. If $I(w) \subseteq \ker \pi_\ell$ for any $w|v$, where $I(w)$ is the inertia subgroup of G attached to w, then we say π_ℓ is unramified at v (or v is unramified with respect to π_ℓ, cf. Serre & Tate [1], p.292. Actually this is so when the condition holds for one w since different $I(w)$ are conjugate). The image of the Frobenius $F(w)$ is defined at this time, and its conjugate class will be denoted by $F(v)_{\pi_\ell}$, which depends only on v. (Sometimes $F(v)_{\pi_\ell}$ will be abbreviated as $F(v)$ only, as its conjugate class is in G.) Let $P(v)_{\pi_\ell}(T)$ denote the characteristic polynomial $\det(1-F(v)_{\pi_\ell}T)$ if v is unramified, where T is an indeterminate. $P(v)_{\pi_\ell}(T)$ is uniquely determined.

2.3. Rationality.

π_ℓ is said to be rational (respectively, integral) if there is a finite set $S \subseteq \sum$ such that

(a) Any places not in S is unramified with respect to

Σ;

(b) If $v \in \Sigma \setminus S$, then $P(v)_{\pi_\ell}(T)$ has coefficients in $\mathbb{Q}$ (respectively, in $\mathbb{Z}$).

S is usually referred to be the exceptional set.

2.4. Compatibility.

Let π_ℓ and $\pi_{\ell'}$ be two ℓ-adic and ℓ'-adic, respectively, representations. They are said to be compatible if there is a finite set $S \subseteq \Sigma$ such that both π_ℓ and $\pi_{\ell'}$ are unramified outside S and $P(v)_{\pi_\ell}(T) = P(v)_{\pi_{\ell'}}(T)$ there.

Compatible representations have many similar propertities, e.g., they have the same kernel. (cf. also prop.17, and MG I-12 for "Questions".)

2.5. Compatibility of a system of ℓ-adic representations.

For each prime number ℓ let π_ℓ be a given ℓ-adic representation. The system (π_ℓ) is said to be compatible if every two π_ℓ's are compatible. Let $S_\ell = \{ v : v|\ell \}$. The system is said to be strictly compatible if there is a finite set $S \subseteq \Sigma$ such that

(a) If $v \notin S \cup S_\ell$ then π_ℓ is unramified at v and $P(v)_{\pi_\ell}(T)$ is of rational coefficients;

(b) $P(v)_{\pi_\ell}(T) = P(v)_{\pi_{\ell'}}(T)$ if $v \notin S \cup S_\ell \cup S_{\ell'}$.

2.6. Semi-simplicity; semi-simplification.

Assume π is a representation of G with representation space V. Let

$$0 = V_n \subseteq V_{n-1} \subseteq \cdots \subseteq V_0 = V$$

be a composition series of G-subspaces. It always exists. Then the representation $\pi^{\wedge}$ associated to

$$(V_0/V_1) \oplus \cdots \oplus (V_{n-1}/V_n)$$

is called the semi-simplification of π (The procedure is valid for any K); it is semi-simple. (MG I §2.3)

If π is a rational ℓ-adic representation, then the semi-simplification $\pi^{\wedge}$ of π is semi-simple, rational, compatible with π (actually they have the same characteristic polynomial). So semi-simplification leaves many properties invariant, e.g., same trace and norm. A representation is to be semi-simple is our basic requirement, because, only base on which many good properties would hold. In case that the representation is not semi-simple, we would like consider its semi-simplification instead. We have

Proposition 1. (thm. MG I §2.3) If π_ℓ is a rational ℓ-adic representation, and ℓ' is another given prime, then there is at most one ℓ'-adic represntation $\pi_{\ell'}$ which is semi-simple, rational, and compatible with π_ℓ.

This is because of the following well known fact (and, the Cebotarev Density Theorem), which is used frequently.

Lemma 2. Two semi-simple finite dimensional representations are isomorphic if they have same trace and, the base field is of characteristic 0.

Compatible semi-simple system is uniquely determined according to the proposition. (So it is natural to ask: will compatible system be strictly compatible?)

2.7. Abelianness.

An Abelian representation factors through G^{ab}. Incidentally, we have

Proposition 2. (corol. of prop.1, MG III §2.2) Any Abelian ℓ-adic representation is unramified outside a finite set of places.

The reason is the reciprocity law (which is essential, cf. § 4 and prop.9 below).

Our latter results will show that we can determine all rational semi-simple Abelian ℓ-adic representations of number fields. This fact has many applications.

2.8. Representation with values in an algebraic group.

We also use the concept of a representation (of G) with values in an algebraic group, where Aut(V) is replaced by an algebraic group H defined over $\mathbb{Q}$ (MG I §2.4). Thus an ℓ-adic representation is a continuous homomorphism π_ℓ: G ——> $H(\mathbb{Q}_\ell)$. Unramifiedness can be similarly defined; rational means the image of the Frobenii is $\mathbb{Q}$-rational or $\mathbb{Q}$ -points. Compatibility is somewhat different. It means, for two representations π_ℓ and $\pi_{\ell'}$ and a place v unramified with respect to both π_ℓ and $\pi_{\ell'}$, that the Frobenii $F(v)_{\pi_\ell}$ and $F(v)_{\pi_{\ell'}}$ have the same evaluation for any central element f of the affine ring of H: $f(F(v)_{\pi_\ell}) = f(F(v)_{\pi_{\ell'}})$ (F(v) : a class!). The meaning will become clear from thm.5-6 of §5.4.

3. Examples.

Here K is any field.

(a) Cyclotomic representations (characters);

The construction. Assume $\ell \neq \mathrm{char}K$. Then G acting on the group μ_n of ℓ^n-th roots of unity in K gives a representation

$$r_n : G \longrightarrow (\mathbb{Z}/\ell^n\mathbb{Z})^\times.$$

Taking inverse limit we have the so-called cyclotomic character

$$\chi_\ell : G \longrightarrow \mathbb{Z}_\ell^\times.$$

Let $T_\ell(\mu) = \varprojlim \mu_n \simeq \mathbb{Z}_\ell$, $V_\ell(\mu) = T_\ell(\mu) \otimes \mathbb{Q}_\ell$. We also write

$$\chi_\ell : G \longrightarrow \mathrm{Aut}(V_\ell(\mu)).$$

The continuity of χ_ℓ comes from a general fact that claims the inverse limit exists in the category of topological groups. (We will apply this fact to the constructions about elliptic curves also.)

Here are some concrete calculations.

$K = \mathbb{Q}$. One has that χ_ℓ is surjective. This comes from the reciprocity for $\mathbb{Q}$ by which we have $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \simeq (\mathbb{Z}^\wedge)^\times$ where $\mathbb{Z}^\wedge = \varprojlim(\mathbb{Z}/n\mathbb{Z}) \simeq \prod \mathbb{Z}_\ell$, cf. Cassels & Frohlich [1], §5 of chap.VII by Tate. The construction is compatible to the above product of $\mathbb{Z}^\wedge$. In particular for each number field K,

$$\chi_\ell : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathbb{Z}_\ell^\times$$

maps $\mathrm{Gal}(\bar{K}/K)$ onto an open subgroup of $\mathbb{Z}_\ell^\times$. For a fixed K, χ_ℓ is surjective for almost all ℓ. It is unramified at each $p \neq \ell$. The Frobenius $F(p)$ in $\mathbb{Z}_\ell^\times$ is exactly p if $K = \mathbb{Q}$; and for general K, Nv instead if v is a place of K not dividing ℓ where Nv is its norm. Hence the system (χ_ℓ) is (rational, in fact integral) strictly compatible with empty exceptional set.

Let's turn to $K = \mathbb{Q}_p$. For each ℓ we have as above

$$\chi_\ell : \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \longrightarrow \mathbb{Z}_\ell^\times .$$

By classfield theory (cf. below), this map is identified with one

$$\chi_\ell : \mathbb{Q}_p^\times \longrightarrow \mathbb{Z}_\ell^\times .$$

It is locally constant if $p \neq \ell$. On the other hand the map $\mathbb{Q}_p^\times \longrightarrow \mathbb{Z}_p^\times$ is surjective. This is again by the reciprocity. In fact, we have $\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \simeq \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$ (Serre [5] p.79) where $\chi_\ell(x) = \ell^\times$ if $x \in \hat{\mathbb{Z}}$ and $\chi_\ell(x) = x$ if $x \in \mathbb{Z}_p^\times$. The reciprocity map is not like the global one. However the global one and the local one are compatible in the sense of §4.4.

(b) ℓ-adic representations obtained from the division points of an elliptic curve defined over K; (for the definitions, cf. Part II §1.)

An elliptic curve gives a system of ℓ-adic representations which is, if K is a number field, rational and strictly compatible with exceptional set contained in the set of places where E has bad reduction. To determine the images of this representations is the main task of Part II. It is not Abelian if E does not have CM; Abelian if E has CM (and all its endomorphisms are) defined over the base field K.

More general

(c) From the division points of an Abelian variety over K;

and

(d) Cohomology representations.

3.0.1 Remark All representations here are essentially of the form (d), cf. Tate [3] §1.

3.1. Elliptic curve over purely transcendental field.

Here is another interesting example.

One can find an elliptic curve E with modular invariant $j=T$, an indeterminate, defined over $\mathbb{Q}(j)$. Then $G_\ell = GL(T_\ell(E))$ (cf. §3 (b)) where $T_\ell(E)$ is the Tate's module of the elliptic curve E (i.e., the representation attached

to E is surjective. For a proof, cf. for example, Robert [1]).

4. Some facts in classfield theory; reciprocity.

4.0. Some notations.

For a field K with a normalized discrete valuation v, write R_v, P_v and U_v the ring of v-integers, the maximal ideal and the group of units of R_v, respectively. Namely,

$$R_v = \{ x \in K : v(x) \geq 0 \};$$
$$P_v = \{ x \in K : v(x) > 0 \};$$
$$U_v = \{ x \in K : v(x) = 0 \}.$$

$k(v) = R_v/P_v$ is the residue field, and $p(v)$ the residue chracteristic (i.e., $\mathrm{char}(k(v))$).

4.1. Decomposition subgroup, inertia subgroup and the Frobenius automorphism.

With the same convention on K, for any finite extension L/K, w a valuation of L extending v, let

$$D(w) = \{ \sigma \in \mathrm{Gal}(L/K) : w \circ \sigma = w \}.$$

This is the decomposition subgroup attached to w. We have a surjective homomorphism

$$D(w) \longrightarrow \mathrm{Gal}(k(w)/k(v))$$

with kernel $I(w)$, the inertia subgroup of w, which is characterized by

$$\sigma(x) \equiv x \pmod{P_w} \qquad \text{for all } x \in R_w$$

In case that $k(w)$ (hence $k(v)$) is finite, $\mathrm{Gal}(k(w)/k(v))$ is generated by the Frobenius automorphism defined by

$$F(w)(x) \equiv x^{Nv} \pmod{P_w} \qquad \text{for all } x \in R_w$$

where $Nv = \#k(v)$ is the norm of v, which is lifted to an $F(w) \in D(w)$ (by abuse of notation) uniquely determined upto modulo $I(w)$.

For another w' extending v, there is a $\sigma \in \mathrm{Gal}(L/K)$ such that $D(w) = \sigma D(w')\sigma^{-1}$. The same is true for $I(w)$ and $I(w')$, and the Frobenii. Write $F(v)$ for the conjugacy class of $F(w)$.

If L/K is infinite, $D(w)$ and $I(w)$, $F(w)$, $F(v)$ can be defined by inverse limit for L'/K runs through all subextensions of L of finite degree. In case that L/K is an Abelian extension (and unramified, i.e., $I(w) = 0$) all these are unique.

4.2. Global reciprocity map.

Assume now K is a number field. $\sum$ is the set of all finite places (or prime ideals, or discrete valuations) of K. $I = I_K$ is the idéle group of K, $C = I/K^\times$ the idele class group (see Weil [2]). Then classfield theory supplies a (topological group) surjective homomorphism (the reciprocity map)

$$C \longrightarrow Gal(K^{ab}/K)$$

with kernel the connected component of C.

4.3. Local reciprocity map.

Let's now turn to the case that K is a local field of characteristic 0, i.e., a finite extension of some $\mathbb{Q}_p$. There is a normalized discrete valuation v on K. Now the local reciprocity map is a continuous homomorphism

$$K^\times \longrightarrow Gal(K^{ab}/K)$$

which induces an isomorphism from U_v to the inertia subgroup $I(v)$ of $Gal(K^{ab}/K)$ and sends a uniformizing element to a Frobenius.

4.4. Relation between local and global.

The global and the local reciprocity maps are compatible in the following sense. If K is a number field, $v \in \sum$ is finite place, K_v the completion of K at v, then we have first an isomorphism

$$D(v)^{ab} \simeq \mathrm{Gal}(K_v^{ab}/K_v)$$

by extension by continuity. On the other hand $K_v^{\times}$ can be viewed as a factor of I: $I = K_v \times I'$. Being so we have

$$\begin{array}{ccc} K_v & \longrightarrow & \mathrm{Gal}(K_v^{ab}/K_v) \\ \downarrow & & \| \\ I & \longrightarrow & \mathrm{Gal}(K^{ab}/K) \supseteq D(v)^{ab} \end{array}$$

In particular we can see which kind of element in I represents a Frobenius.

We will hereafter, within this chapter, work on local and global fields of characteristic 0 unless otherwise stated.

5. The representation attached to a Serre's torus.

Refernce: MG II. There is a standard method to construct Abelian ℓ-adic representations of number fields, due to Serre, namely via the "Serre's tori".

5.1. The construction of the algebraic groups T_m and S_m.

Here are some notations. Let K be a number field, O its ring of integers, E the group of units of O. I is the idéle group and C the idele class group of K; K_v the completion of K at v with R_v, P_v, U_v exactly as mentioned in §4.0.

$m = \{ m_v \}$ is a "module", i.e., a finite set of positive integers m_v where $v \in S$ and $S \subseteq \sum$ is a finite set. S is referrd to be the support. Let

$$(2) \qquad U_{v,m} = \begin{cases} \text{connected component of 1, if } v \text{ infinite;} \\ \{ u \in U_v : \operatorname{ord}(1-u) > m_v \}, \text{ if } v \in S; \\ U_v, \text{ if } v \notin S \ \& \ v \text{ finite.} \end{cases}$$

$U_m = \prod U_{v,m}$; this is an open subgroup of I. $E_m = E \cap U_m$. (Note $[E:E_m] < \infty$) $I_m = I/U_m$, $C_m = I/(K^\times U_m)$. C_m is finite.

Being these ready, we have an exact sequence:

$$1 \longrightarrow K^\times/E_m \longrightarrow I_m \longrightarrow C_m \longrightarrow 1.$$

Let $T = R_{K/\mathbb{Q}}(G_m)$, the torus obtained from the multiplicative group $G_m = GL(1)$ by restricting the scalar field from K to $\mathbb{Q}$ (cf. Weil [1] §1.3), $T_m = T/\overline{E_m}$ where $\overline{E_m}$ means the Zariski closure. We can then construct the algebraic group S_m for the morphism $K^\times/E_m \longrightarrow T_m(\mathbb{Q})$ as an extension of T_m

5.1. The construction of the algebraic groups T_m and S_m.

Here are some notations. Let K be a number field, O its ring of integers, E the group of units of O. I is the idéle group and C the idele class group of K; K_v the completion of K at v with R_v, P_v, U_v exactly as mentioned in §4.0.

$m = \{ m_v \}$ is a "module", i.e., a finite set of positive integers m_v where $v \in S$ and $S \subseteq \sum$ is a finite set. S is referrd to be the support. Let

$$(2) \qquad U_{v,m} = \begin{cases} \text{connected component of 1, if } v \text{ infinite;} \\ \{ u \in U_v : \operatorname{ord}(1-u) > m_v \}, \text{ if } v \in S; \\ U_v, \text{ if } v \notin S \ \& \ v \text{ finite.} \end{cases}$$

$U_m = \prod U_{v,m}$; this is an open subgroup of I. $E_m = E \cap U_m$. (Note $[E:E_m] < \infty$) $I_m = I/U_m$, $C_m = I/(K^\times U_m)$. C_m is finite.

Being these ready, we have an exact sequence:

$$1 \longrightarrow K^\times/E_m \longrightarrow I_m \longrightarrow C_m \longrightarrow 1.$$

Let $T = R_{K/\mathbb{Q}}(G_m)$, the torus obtained from the multiplicative group $G_m = GL(1)$ by restricting the scalar field from K to $\mathbb{Q}$ (cf. Weil [1] §1.3), $T_m = T/\overline{E_m}$ where $\overline{E_m}$ means the Zariski closure. We can then construct the algebraic group S_m for the morphism $K^\times/E_m \longrightarrow T_m(\mathbb{Q})$ as an extension of T_m

by the finite group C_m (cf. MG II §2):

$$1 \longrightarrow T_m \longrightarrow S_m \longrightarrow C_m \longrightarrow 1$$

to which we have the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times/E_m & \longrightarrow & I_m & \longrightarrow & C_m & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & T_m(\mathbb{Q}) & \longrightarrow & S_m(\mathbb{Q}) & \longrightarrow & C_m & \longrightarrow & 1 \end{array} \tag{3}$$

with the first square a push-out (cf. II, loc. cit.). S_m is of multiplicative type because it is an extension of a torus by a finite group.

5.2. The canonical representation $\mathcal{E}_\ell$.

First by taking $\mathbb{Q}_\ell$-points we have

$$\pi_\ell : T(\mathbb{Q}_\ell) \longrightarrow T_m(\mathbb{Q}_\ell) \longrightarrow S_m(\mathbb{Q}_\ell),$$

so we have

$$\alpha_\ell : I \longrightarrow T(\mathbb{Q}_\ell) \xrightarrow{\pi_\ell} S_m(\mathbb{Q}_\ell).$$

from the projection $I \longrightarrow \prod_{v \mid \ell} K_v^\times = T(\mathbb{Q}_\ell)$. On the other hand

$$\mathcal{E} : \quad I \longrightarrow I_m \longrightarrow S_m(\mathbb{Q}).$$

Diagram (3) shows $\mathcal{E}$ and α_ℓ coincide on $K^\times$, so if we put

$\mathcal{E}_\ell(x) = \mathcal{E}(x) \cdot \alpha_\ell(x^{-1})$ for $x \in I$ we have the map

(4) $\mathcal{E}_\ell : C \longrightarrow S_m(\mathbf{Q}_\ell)$.

where $C = I/K^\times$ is the idele class group. $\mathcal{E}_\ell$ is continuous for the ℓ-adic topology on $S_m(\mathbb{Q}_\ell)$. This is because that π_ℓ is an algebraic group morphism hence it is continuous for the ℓ-adic topology, so is α_ℓ; and on the other hand $\mathcal{E}$ is locally constant. According to classfield thory this can be identified with a map of G^{ab} since $S_m(\mathbf{Q}_\ell)$ is totally disconnected as an ℓ-adic Lie group and $\mathcal{E}_\ell$ is hereof trivial on the connected component of C (see §4.2). We (will always) abuse an Abelian ℓ-adic representation of K as a map on either I or C or G^{ab}, particularly for $\mathcal{E}_\ell$ by this reason. $\mathcal{E}_\ell$ is then a representation of K with values in the algebraic group S_m, cf. §2.8.

Remark Our construction is natural with respect to the module m.

5.3. The property of $\mathcal{E}_\ell$.

Let f_v be an idéle which is a uniformizing element at v, $F(v) = \mathcal{E}(f_v)$. (The notation will be seen reasonable from the theorem below.) Note $F(v)$ is independent of f_v if $v \notin \mathrm{supp}(m)$.

Theorem 3. (prop., MG II §2.3) $\mathcal{E}_\ell$ is rational and un-

ramified at all $v \notin \mathrm{supp}(m) \cup S_\ell$ with Frobenius $F(v) \in S_m(\mathbb{Q})$. The ξ_ℓ's form a system of representations with values in the algebraic group S_m which is strictly compatible with exceptional set contained in supp(m).

Proof. Immediately from the constuction.

Each representation ξ_ℓ brings imformation, for

Proposition 4. (lemma, MG II §2.4) The set of Frobenii $F(v)$ where $v \in \Sigma$ is dense in S_m for the Zariski topology.

Proof. That set is dense in $S_m(\mathbb{Q}_\ell)$ for the ℓ-adic topology, so its ℓ-adic closure $X = \overline{\mathrm{im}(\xi_\ell)}$ in $S_m(\mathbb{Q}_\ell)$. But $\mathrm{im}(\xi_\ell)$ contains an ℓ-adic open set which is always Zariski dense, hence the result.

5.4. The ℓ-adic representation associated to a linear representation of S_m.

For an prime ℓ, if $\phi: S_m \longrightarrow GL_V$, here V is a $\mathbb{Q}_\ell$-vector space of some dimension n and GL_V means the algebraic group $GL(n)$ over $\mathbb{Q}_\ell$, is a linear representation of S_m defined over $\mathbb{Q}_\ell$, then

(5) $\phi_\ell = \phi \circ \xi_\ell : G^{ab} \longrightarrow \mathrm{Aut}(V)$

is an Abelian ℓ-adic representation of the number field K.

We have

Theorem 5. (prop., MG II §2.5) It is semi-simple and unramefied at each $v \notin \text{supp}(m)\ S$ with Frobenius $\phi(F(v))$. It is rational iff ϕ can be defined over $\mathbb{Q}$.

Proof. The semi-simplicity comes from that of S_m, since S_m is of multiplicative type, see also prop.4. For the Frobenius, note ξ is trivial on U_m. Finally if ϕ_ℓ rational, as $F(v)$ is a priori a $\mathbb{Q}$-point, rationality will imply that $\phi(F(v))$ is also a $\mathbb{Q}$- point. Then prop.4 applies to complete the proof.

5.4.1 If we have $\phi : S_m \longrightarrow GL_V$ defined over $\mathbb{Q}$ as an algebraic morphism, then we will have a system (ϕ_ℓ) of representations, as defined in (5).

Theorem 6. (thm. MG II § 2.5) The system is Abelian rational semi-simple and strictly compatible with exceptional set contained in supp(m). The Frobenii are $\phi(F(v))$. We also notice that for infinitely many ℓ, ϕ_ℓ is brought into diagonal form.

Proof. The last part is because that there are so many places of degree 1, i.e. split completely, in any finite extension of K. On the other hand S_m (or ϕ) is itself brought into diagonal form in some finite extension of K.

6. Characters of T_m.

In order to construct the desired ℓ-adic representations, we must consider the linear representations of S_m. But S_m is of multiplicative type, its representations are given by its characters over K. We have known much about its character group. Let X denote the character group.

6.1. Characters related to that of T.

(cf. again MG II §3) $X(T)$, the character group of T, is generated by the $[\sigma]$'s, where $\sigma \in \overline{\Gamma}$, the set of all embeddings of K into $\overline{\mathbb{Q}}$ and the $[\sigma]$'s are being considered as characters by extension of scalar field. So the characters of T_m are of the form

$$\phi = \prod_{\overline{\Gamma}} [\sigma]^{n(\sigma)}$$

for some integers $n(\sigma)$ which satisfy

$$\phi(x) = \prod_{\overline{\Gamma}} \sigma(x)^{n(\sigma)} = 1 \qquad \text{for } x \in E_m$$

6.2. Some formulas.

In view of our push-out construction (cf. (3) of §5.1), a character Θ of S_m is identified with a pair (ϕ, f) where $\phi \in X(T)$ and $f \in \mathrm{Hom}(I, \bar{\mathbf{Q}}^\times)$ satisfying

(a) $f(x) = 1$ for $x \in U_m$;

(b) $f(x) = \phi(x)$ for $x \in K^\times$.

(Note that the condition of §6.1 on ϕ is naturally satisfied: $E_m = K \cap U_m$, i.e., $\phi \in X(T_m)$.) This amounts to the same, together with §6.1, as for some g:

$$g: I \longrightarrow \bar{\mathbb{Q}}^\times$$

satisfying

(a)' $g(x) = 1$ for $x \in U_m$;

(b)' $g(x) = \prod_\tau \sigma(x)^{n(\sigma)}$ if $x \in K = T(\mathbb{Q})$

for some integers $n(\sigma)$. The relation between Θ and g is: $g = \Theta \cdot \xi$ for ξ in §5.2 (this relation also holds for higher dimensional linear representations). Note from $0 \longrightarrow T_m \longrightarrow S_m \longrightarrow C_m \longrightarrow 0$, one has $0 \longrightarrow X(C_m) \longrightarrow X(S_m) \longrightarrow X(T_m) \longrightarrow 0$ exact. Hence each $\phi \in X(T_m)$ can be extended to a $(\phi, f) \in X(S_m)$. Whereas characters of S_m are in a one-one correspondence to the pairs (ϕ, f), and to the g's.

6.3. Example: the case $K = \mathbb{Q}$, $S = \phi$.

Now $U = \mathbb{R}^+ \times \prod U_p$, $E = \{\pm 1\}$, $E_m = \{1\}$, $T = S = G_m$. Also $C_m = C/\mathbb{Q}^\times U = \{1\}$ since $\mathbb{Z}$ is of class number 1. $I = \mathbb{Q}^\times U$ and $I_m = I/U = \mathbb{Q}^\times$. We then omit the subscript "m" as in §5.1-2. Our diagram (3) becomes trivial now

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Q}^\times & \longrightarrow & \mathbb{Q}^\times & \longrightarrow & 1 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{Q}^\times & \longrightarrow & \mathbb{Q}^\times & \longrightarrow & 1 & \longrightarrow & 1. \end{array}$$

The data being ready, consider

$$\xi_\ell : I \longrightarrow S(\mathbb{Q}_\ell) = \mathbb{Q}_\ell^\times$$

One has, if $a = (a_p) \in I$,

$$\xi(a) = \operatorname{sgn}(a_\infty) \prod p^{v_p(a_p)} = \gamma,$$

where $a = u \cdot \gamma$ with $\gamma \in \mathbb{Q}^\times$, $u \in U$, following the direct product decomposition $I = U \cdot \mathbb{Q}^\times$. As obviously $\alpha_\ell(a) = a_\ell$, we see

$$\xi_\ell(a) = \gamma \cdot a_\ell^{-1} \qquad \text{if} \quad a = (a_p) = u \cdot \gamma \in I$$

In particular $F(p) = p$ with the notation as in §5.3. Therefore ξ_ℓ coincides with the cyclotomic character χ_ℓ. (This follows from the Cebotarev Density Theorem (cf. lemma 1).)

A little bit more general, we construct a character

$$N : S_m \longrightarrow G_m$$

for any number field K which sends $F(v)$ to $Nv \in \mathbb{Q}^\times$. This map is unique whenever it exists, by prop.4. In fact, if there is a set of elements $a_v \in \mathbb{Q}^\times$ and an algebraic morphism

$h: T \longrightarrow G_m$ such that

$$h(\alpha) = \prod_v a_v^{v(\alpha)} \qquad \text{for all } \alpha \in K^\times \text{ such that } \alpha \equiv 1 \pmod{m^\times}$$

(Note in view of (2) of §5.1 this implies $\alpha > 0$ at any real places.) then we can define a character Θ of S_m such that $\Theta(F(v)) = a_v$ as follows. First h factors through T_m, because E_m satisfies the condition for the above formula and $v(\alpha) = 0$ for any v and any $\alpha \in E_m$. Then we extend h to a Θ' in $X(S_m)$. Let $t = \#C_m$. Then

$$\Theta'(F(v))^t = \Theta'(F(v)^t) = \prod_{v'} a^{tv'(F(v))} = a_v^t$$

since $F(v)^t \in K^\times \cap U_m$. ($v'(F(v)) = 1$ if $v' = v$ and 0 otherwise, see the definition of $F(v)$ at §5.3) One finds Θ' differs from our desired Θ by a character of C_m. (Note the exact sequence $0 \longrightarrow X(C_m) \longrightarrow X(S_m) \longrightarrow X(T_m) \longrightarrow 0$ splits. In fact, $X(T)$ is free, hence so is $X(T_m) \subseteq X(T)$.)

The 1-dim representation attached to N, denoted again by ξ_ℓ, maps the Frobenius $F(v)$ for each $v \nmid \mathrm{supp}(m)$ to Nv. So again by Cebotarev's Density Theorem ξ_ℓ coincides with the cyclotomic character of K (or $\mathrm{Gal}(\overline{K}/K)$), see for instance example (a) of §3.1.

6.4. Another formula.

For $v \in \Sigma$ lying over ℓ, choose a place v_ℓ of $\overline{\mathbf{Q}}$ extending v so that one has a completion map:

$$\overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}_\ell$$

corresponding to this v_ℓ. Define

$$\sigma_\ell : K_\ell \longrightarrow \overline{\mathbb{Q}}_\ell$$

via

$$K_\ell \longrightarrow K_v \longrightarrow \overline{\mathbb{Q}}_\ell$$

where v is the unique place such that $v = v_\ell \circ \sigma$ restricted on K.

If $\phi \in X(T)$ which is of the form

$$\phi = \prod_{\Gamma} [\sigma]^{n(\sigma)}$$

(cf. §6.1) we can define ϕ_ℓ by the formula

$$\phi_\ell(x) = \prod \sigma_\ell(x)^{n(\sigma)} \qquad \text{for } x \in K_\ell^\times$$

which is just the extension of ϕ on T by scalar extension from $\mathbb{Q}$ to $\mathbb{Q}_\ell$.

Being so, for $\tilde{\Phi} = (\phi, f) \in X(S_m)$ (cf. §6.2), put $\tilde{\Phi}_\ell(a) = f(a) \cdot \phi_\ell(a_\ell^{-1})$ where $a \in I$ and a_ℓ is the ℓ-th component of a. $\tilde{\Phi}_\ell$ is a character from I to $\mathbb{Q}_\ell^\times$ which is just the character associated to the character $\tilde{\Phi}$ of S_m in the sense of §5.2. One has

$$\tilde{\Phi}_\ell(a) = \phi_\ell(a_\ell^{-1}) = \prod \sigma_\ell(a)^{n(\sigma)} \qquad \text{if } a \in U_m$$

7. Struucture of $X(T_m)$.

We are to look into more detail of $X(T_m)$. Write $X(T)$ additive; put $Y(T) = X(T)\otimes\mathbb{Q}$. Let C be the set of all "Frobenii at infinity": for each complex place w, the decomposition group is of order 2, then the non-trivial element is the corresponding "Frobenius" (= complex conjugate). And

$$Y = \mathbb{Q}\,(\sum_{\Gamma}[\sigma]);$$
$$Y = \{\sum_{\Gamma} b_\sigma[\sigma] : b_\sigma\in\mathbb{Q},\ \sum b_\sigma = 0,\ b_\sigma = -b_{c\sigma} \text{ for } c\in C\}$$
$$Y^- + Y^+ = \{\sum_{\Gamma} b_\sigma[\sigma] : b_\sigma\in\mathbb{Q},\ \sum b_\sigma = 0\}$$

where Γ is the set of all embeddings of K into $\overline{\mathbb{Q}}$. Then

$$Y(T) = Y^\circ \oplus Y^- \oplus Y^+ \quad \text{and} \quad Y(T_m) = Y^\circ \oplus Y^-.$$

This fact is obtained by the technique of "killing arithmetic subgroups (here is E_m) in a torus", cf. MG Appendix of II.

Now if $\chi \in X(T_m) \subseteq X(T)$ and $\chi = a(\sum[\sigma]) + (\sum b_\sigma[\sigma])$ where $a,\ b_\sigma\in\mathbb{Q}$, then we have $a+b_\sigma\in\mathbb{Z}$, $\sum b_\sigma = 0$, and $2a\in\mathbb{Z}$ (hence $2b_\sigma\in\mathbb{Z}$). In particular we have a homomorphism:

(6) $\quad j: X(T_m) \longrightarrow \mathbb{Z}$ via $\chi \longmapsto 2a.$

7.1. The Frobenius.

(MG II §3.4) One of the basic questions to study the Galois representation is to calculate the eigenvalues of the Frobenii. We indicate a technique to calculate related data of the Frobenius, e.g. the theorem of §7.2 below. That result has been desired.

When a linear representation Φ of S_m is given, its restriction on T_m can be brought into diagonal form in a finite extension of K, hence given by characters $\chi_1, \cdots, \chi_n$ such that we can write

$$\chi_i = \sum_{\tau} n_\sigma(i)[\sigma].$$

Now there is an integer t such that $F(v)^t \in T_m(\mathbb{Q})$ for all $F(v)$ since S_m/T_m is finite. If $\mathfrak{p}_v$ is the prime ideal of K at v then

$$\mathfrak{p}_v^t = (\alpha)$$

with $\alpha \equiv 1 \pmod{m^\times}$ and α is totally positive (cf. Definition of U_m). The eigenvalues of $\Phi(F(v)^t)$ is then obviously given by $\chi_i(\alpha) = \prod \sigma(\alpha)^{n_\sigma(i)}$ (In particular the eigenvalues of $\Phi(F(v))$ are $\mathfrak{p}_v$-units, i.e., a w-unit whenever $w \nmid v$)

7.2. The Frobenius (cont'd).

Let $z_1, \cdots\cdots, z_n$ be eigenvalues of $\Phi(F(v))$ such that $z_i^t = \chi_i(\alpha)$. Let $w|v$ be an extension of v to $\bar{K}$. Then

$$w(z_i) = \sum_{\Gamma(v)} n_\sigma(i) \qquad \text{where } \Gamma(v) = \{ \sigma : w\circ\sigma = v \}$$

as we know $w(z_i) = \sum n_\sigma(i) w\circ\sigma(\alpha)$ summing over Γ and

$$w\circ\sigma(\alpha) = \begin{cases} 0 & \text{if } w\circ\sigma \neq v \\ N & \text{if } w\circ\sigma = v. \end{cases}$$

Theorem 7. (prop., MG II § 3.4) Let $v \notin \text{supp}(m)$ and χ be a character of S_m. Let χ_T $X(T_m)$ be the restriction of χ to T_m and $i = j(\chi_T)$ be the integer defined in (6) of §7.0 above. Then for any Archimedian valuation w of $\mathbb{Q}$, we have $w(\chi(F(v)) = (Nv)^{i/2}$.

Proof. Write, cf. §7.0,

$$\chi = a(\sum_\Gamma [\sigma]) + (\sum_\Gamma b_\sigma [\sigma])$$

then $i = j(\chi_T) = 2a$. Now

$$(7) \qquad w(\chi(F(v))^t) = w(\chi(F(v)^t)) = (\prod_\Gamma w\circ\sigma(\alpha))^a (\prod_\Gamma w\circ\sigma(\alpha)^{b_\sigma})$$

where $(\alpha) = \mathfrak{P}_v^t$, see §7.1. But $\prod w\circ\sigma(\alpha)^a = w(N(\alpha)) = (N(v))^{it/2}$ as $(\alpha) = \mathfrak{P}_v^t$. And if $c \in C$ attached to w (i.e., the one such that $w\circ c = w$) then, as $c\Gamma = \Gamma$

$$\prod_{\Gamma} w\circ\sigma(\alpha)^{b_\sigma} = \prod_{\Gamma} w\circ c\circ\sigma(\alpha)^{b_{c\sigma}} = \prod w\circ\sigma(\ )^{b_{c\sigma}}$$

the product of the two sides is 1 since $b_\sigma+b_{c\sigma}=0$, this shows each factor is 1, i.e., the second factor on the right hand side of (7) is 1. That concludes our assertion.

8. Local algebraicity.

There is another description of the Abelian representations defined in §5, namely the local algebraicity. The above considered Abelian representations are locally algebraic; conversely, an Abelian rational semi-simple locally algebraic representation is induced in the above way (§5). There are other methods to detect local algebraicity (e.g. Hodge-Tate module; or when the base field K is of particular form), which will bring great convenience because of our knowledge from algebraic geometry.

8.1. Local case.

K is here a finite extension of $\mathbb{Q}_p$. $G^{ab} = \mathrm{Gal}(K^{ab}/K)$. Let

$$\pi : G^{ab} \longrightarrow \mathrm{Aut}(V)$$

be an Abelian p-adic representation where V is a finite

dimensional vector space over $\mathbb{Q}_p$. Let $T=R_{K/\mathbb{Q}}(G_m)$. According to local classfield theory (see § 4.3) we identify π as a map

$$\pi : K^{\times} \longrightarrow G^{ab} \longrightarrow \mathrm{Aut}(V).$$

Say π locally algebraic if there is an algebraic group morphism

$$r: T \longrightarrow GL_V$$

where $GL_V = GL(n)$, if $n=\dim V$, is the general linear group viewed as an algebric group over $\mathbb{Q}_p$, such that $\pi(x) = r(x^{-1})$ for all $x \in K^{\times}$ closed to 1.

The restriction of a locally algebraic ℓ-adic representation π to the inertia is always semi-simple. In fact π restricted to an open neighbourhood of 1 in U_p, the group of units of K, which is just $1/r$, is semi-simple, noting T is of multiplicative type. But U_p is compact, the semi-simplicity of π on U_p is now derived from a standard average argument (MG III §1.1, prop.1) . Conversely if furthermore the G-module V is of "Hodge-Tate Type", then the representation is locally algebraic. (cf. MG III §1 & Appendix; also §8.5 below)

When the restriction of π to the inertia group (or U_p) is diagonalizd by characters χ_i over $\overline{K}$, we have

Proposition 8. (MG III §1.1, prop.2) π is locally algebraic iff the χ_i look like characters of the algebraic group T, i.e., (as usual $\overline{T}$ = the set of embeddings of K into $\overline{\mathbb{Q}}$)

$$\chi_i(u) = \prod_{\overline{T}} \sigma(u)^{-n_\sigma(i)}$$

for some integers $n_\sigma(i)$ and for $u \in K^\times$ closed to 1.

Let's consider the case when $K = \mathbb{Q}_p$. A character

$$\mathrm{Gal}(K^{ab}/K) \longrightarrow U_p = GL(1,\mathbb{Z}_p)$$

identified, when restricted to the inertia, with a map

$$\rho : \mathbb{Q}_p^\times \longrightarrow U_p$$
$$\uparrow \nearrow$$
$$U_p$$

according to local reciprocity, is of the form $\rho(x) = x^v$ for some $v \in \mathbb{Z}_p$ (by a continuity argument, similar to the transcendental case for multiplicative functions), valid for x in an open subgroup of U_p (= the inertia). Hence, consequently, ρ is locally algebraic iff $v \in \mathbb{Z}$.

8.2. Global case.

Let

$$\pi_\ell : \mathrm{Gal}(K^{ab}/K) = G^{ab} \longrightarrow \mathrm{Aut}(V_\ell)$$

be an ℓ-adic representation of a number field K where V_ℓ is finite dimensional vector space over $\mathbb{Q}_\ell$. For $v|\ell$ let $D(v)^{ab}$ be the decomposition group in G^{ab} attached to v. Then we have

$$\pi_v : \mathrm{Gal}(K_v^{ab}/K_v) \simeq D(v)^{ab} \longrightarrow \mathrm{Aut}(V_\ell).$$

Say π_ℓ is locally algebraic iff π_v is so for all $v|$. Let

$$i_\ell : K^\times \longrightarrow I \longrightarrow G^{ab}.$$

We have, π is locally algebraic iff there is an algebraic morphism

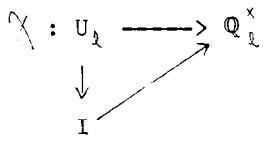
$$f : T \longrightarrow GL_V \qquad \text{defined over } \mathbb{Q}_\ell,$$

such that $\pi_\ell \circ i_\ell(x) = f(x^{-1})$ for $x \in K_\ell^\times$ closed to 1. We say that π is with associated morphism f. It is unique (again by prop.4). (MG III § 2)

8.3. An example.

Consider the case $K = \mathbb{Q}$ and $\pi : I \longrightarrow \mathrm{Aut}(V)$ is the Abelian locally algebraic ℓ-adic representation associated to $f: G = T \longrightarrow GL_V$. Since $f = \coprod [\sigma] : G \longrightarrow GL_V$ where $\sigma : \mathbb{Q} \longrightarrow \mathbb{Q}$ is the identity, the only element of

Γ (i.e. completely reducible), f is given by characters χ . Let's turn to consider 1-dimensional representations. The restriction of a character to the inertia



satisfies

$$\chi(x) = \sigma(x)^{-m}$$

for some integer m and for x closed to 1. Here the map σ is no other than the cyclotomic character χ_ℓ, by considering the iamge of the Frobenii by usual identification, cf. §3. Now $\chi \cdot \chi_\ell^m$ is trivial on some open subgroup of U_ℓ. It is certainly locally trivial on each U_p, and on the whole U_p for almost all p by unramified property (cf. prop.2.). So $\chi \cdot \chi_\ell^m$ factors through

$$I/(\mathbb{Q}^\times \times \mathbb{R}^+ \times (\prod_{\text{a.a.p}} U_p) \times (\prod_{\text{other p}} U'_p))$$

where U'_p is some open subgroup of U_p and "a.a." means here "almost all". This is a finite group. That means, χ differs from χ_ℓ^{-m} by a character of finite order.

8.4. Module of local algebraicity; the equivalence of locally algebraic representation and that associated to Serre's

torus; the theorem of Serre and Lang.

Again K is a number field and assume that π is a locally algebraic ℓ-adic representation of K. To relate to the representations associated to tori, we have the "module of local algebraicity". For such a module $m = \{m_v\}$ of definition, if π associated to f, then (see (2) of §5.1)

(a) π is trivial on $U_{v,m}$ when $v \nmid \ell$;
(b) $\pi \cdot i_\ell(x) = f(x^{-1})$ for any $x \in \prod U_{v,m} = U_m$

One sees, by a fact which asserts that every continuous homomorphisms from an ℓ-adic Lie group to another ℓ'-adic Lie group is always locally constant if $\ell \neq \ell'$ (MG III §2.2 prop.), that:

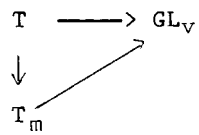
Proposition 9. (MG III §2.2, prop.2) Every locally algebraic representation has a module of definition.

Proof. Because of prop.2, supp(m) can be finite. By the above quoted assertion, enlarge m if necessary one sees (a) of §8.4 is satisfied. For (b), we refer to the definition of local algebraicity.

8.4.1 If $\pi = \phi_\ell$ is the ℓ-adic representation associated to $\phi : S_m \longrightarrow GL_V$ defined over $\mathbb{Q}$ via a Serre's torus S_m then π is (clearly) locally algebraic with associated morphism ϕ and module m. Conversely

Theorem 10. (MG III §3.4) A locally algebraic rational ℓ-adic representation π comes from a Serre's torus associated to some $\phi : S_m \longrightarrow GL_V$ defined over $\mathbb{Q}$.

Proof. If f associated with π, then f factors through



if m is a module of defenition by prop.9. In view of the push-out (3) this gives a ϕ on S_m. ϕ is in fact defined over $\mathbb{Q}$ because of the rationality of π, cf. proof of thm.5 in §5.4. Finally that ϕ induces π is a routine verification.

Hence particularly for this π, there is a system (π_ℓ) of rational semi-simple Abelian representations, compatible with π, and this system is strictly compatible. This important fact will be used later. (cf. §4.4) Consequently all eigenvalues of the Frobenii generate a finite extension over $\mathbb{Q}$!

8.4.2 When the base field is simple the answer is quite beautiful. It is expected that the same result will hold even if that there is no assumption on K (MG p.III-20, Remark (2)).

Theorem 11. (MG thm. of III §3) Assume $K = \mathbb{Q}$ or compositum of quadratic extensions of $\mathbb{Q}$. Then every rational semi-simple Abelian ℓ-adic representation is locally algebraic.

Proof. MG III.

8.5. Tate's theorem.

We exhibite some facts about Hodge-Tate module. (Reference: MG III, Serre [10] and Tate [1]) Assume K is a finite extension of $\mathbb{Q}_p$ with residue field k. Let C be the completion of the algebraic closure of K. Then $G = \mathrm{Gal}(\overline{K}/K)$ acts continuously on C (by continuity).

For a finite dimensional C-vector space W which is also a Galois module by $\sigma(c \cdot x) = \sigma(c) \cdot \sigma(x)$ for $\sigma \in G$, we let

$$X^i = \{ x \in W : \sigma(x) = \chi_p(\sigma)^i x \}, \qquad X(i) = X^i \otimes C.$$

Then Tate proves

Theorem The map $\xi : \coprod_i X(i) \longrightarrow W$ is injective.

We say that W is of Hodge-Tate type if ξ is an isomorphism. For a Galois module V over K by

$$\pi : G \longrightarrow \mathrm{Aut}(V)$$

set $W = V \otimes C$. Say π is of Hodge-Tate type if W is so.

The decomposition for such a V reflects the action π. We have the following celaborated theorem of Tate:

Theorem Assume π is Abelian. Then π is locally algebraic iff it is semi-simple when restricted to the inertia subgroup and is of Hodge-Tate type.

9. The relation with the reduction.

9.1. A lifting theorem of Serre. (Reference: Serre [8] §3)

As before $\xi_\ell : G^{ab} \longrightarrow S_m(\mathbb{Q}_\ell)$ (see (4) of §5.2 and the notations there). Let $\phi_\ell : G^{ab} \longrightarrow \mathbf{Q}_\ell^\times$ be associated with a character $\phi : S_m(\mathbf{Q}_\ell) \longrightarrow \mathbb{Q}_\ell^\times$. As G^{ab} is compact the image is in the group of units of $\mathbb{Q}_\ell$. So reduction gives

$$\tilde{\phi_\ell} : G^{ab} \longrightarrow k^\times,$$

"the character modulo ℓ". The image is always finite, being compact and discrete. By §6.4, we have necessarily

$$\tilde{\phi_\ell}(a) = \prod \sigma_\ell(\tilde{a_\ell^{-1}})^{n(\sigma)} \qquad a \in U_m$$

for some integers $n(\sigma)$. Conversely, let L be an infinite set of prime numbers (meaning "only 0 can be divisible by infititely many primes"), if for each $\ell \in L$ a character

$$\Theta_\ell : G^{ab} \longrightarrow k^\times$$

is given, (recall that we have abused Θ as a map from either G^{ab} or I, with latter the idéle group) then we have the following lifting theorem of Serre:

Theorem 12. (Serre [8] prop.20) Suppose there is a set of integers $\{ n(\sigma,\ell) : \sigma \in \Gamma, \ell \in L \}$ such that

(a) All $n(\sigma,\ell)$ are bounded by an integer N, independent of σ and ℓ;

(b) For all $\ell \in L$, $a \in U_m$, we have
$$\Theta_\ell(a) \equiv \prod \sigma_\ell(a)^{n(\sigma,\ell)} \quad (\bmod \ell)$$

Then there exists a $\Theta \in X(S_m)$ such that that $\Theta_\Gamma = \Theta_\ell$ for infinitely many times.

Proof. The first step is to replace L by a smaller subset, but still infinite, such that the $n(\sigma,\ell)$ are independent of σ. This is possible as the σ's are finitely many and the $n(\sigma,\ell)$ are bounded by N. Then the character

$$\Phi = \prod [\sigma]^{n(\sigma)}$$

is related to our lifting. In fact, first we can prove that

it is a character of T_m (just to show that ϕ vanishes at E_m) by (b), then it extends to one on S_m, still denoted by ϕ . ϕ differs from each θ_ℓ by some roots of unity within some order. The difference can be chosen to be independent of ℓ for infinitely many times, which is again given by a character of C_m (see §6.3.).

Remark Condition (b) is paralell to that of unramifiedness.

Moreover,

Theorem 13. (Serre [8] §3.6 thm.1) Suppose (π_ℓ) is a strictly compatible system of semi-simple rational ℓ-adic representations. Assume that there is an infinite set L of prime numbers such that, if $\ell \in L$, the semi-simplification $\tilde{\pi_\ell}$ of the reduction of π_ℓ is Abelian, and is given by characters $\theta_\ell^{(i)}$, satisfying the following condition:

(*) There are integers $n(\sigma,\ell,i)$, bounded by an integer N, such that

$$\theta_\ell^{(i)}(a) \equiv \prod \sigma_\ell(a_\ell^{-1})^{n(\sigma,\ell,i)} \pmod{\ell} \quad \text{for all } a \in U_m.$$

Then the system (π_ℓ) is isomorphic to a system (ϕ_ℓ) associated with some $\phi : S_m \longrightarrow GL_V$ as defined in §5. In particular, (π_ℓ) is Abelian.

Proof. We can lift $\tilde{\pi_\ell}$ for infinitely many times to a ϕ,

and ϕ is diagonalized. Condition (*) then implies ϕ is a rational representation defined over $\mathbb{Q}$ compatible with (π_ℓ), hence the result.

9.2. Tame inertia: the exact image. (Reference: Serre [8] §1)

We take some explicit consideration for the local case. Here we only assume that K is complete with respect to some discrete valuation. Let $p=\mathrm{chark}$ be the residue characteristic.

Let $K_s \supseteq K_t \supseteq K_{nr} \supseteq K$ where K_{nr} is the maximal unramified extension of K, K_t the maximal tamely ramified extension. Put (in this subsection)

$$G = \mathrm{Gal}(K_s/K), \quad I = \mathrm{Gal}(K_s/K_{nr}), \quad I_p = \mathrm{Gal}(K_s/K_t).$$

Hence $G \supseteq I \supseteq I_p$. Here I is the inertia group; I_p is the p-inertia which is the maximal profinite p-group in I. And

$$I_t \overset{\Delta}{=} I/I_p \approx \mathrm{Gal}(K_t/K_{nr})$$

will be called the tame inertia group, according to Serre.

Let x be a uniformizing element of K_{nr}. For each integer d, $(d, p)=1$, put $K_d = K_{nr}(\sqrt[d]{x})$. Then

$$\Theta_d : \mathrm{Gal}(K_d/K_{nr}) \longrightarrow \mu_d$$

defined by $s(\sqrt[d]{x}) = \theta_d(s)\sqrt[d]{x}$ for $s \in \mathrm{Gal}(K_d/K_\pi)$ is an isomorphism. θ_d is clearly the character corresponding to the Kummer extension. As $K_t = \cup K_d$, one has

$$I_t = \mathrm{Gal}(K_t/K_\pi) \approx \varprojlim \mathrm{Gal}(K_d/K_\pi) \approx \varprojlim \mu_d.$$

9.2.1 The consideration of I_t is natural.

Proposition 14. (Serre [8] prop.4) A semi-simple representation of G in a finite dimensional vector space over any field is trivial on I_p.

Proof. Consider only that a π which is simple. As explained above $\pi(I_t)$ is always a finite p-group, its invariant space $V' \neq 0$ by counting the number of its points which is $\equiv 0 \pmod p$, cf. Serre [5] p.146, thm.2. But I_p is normal so V' is a G-invariant space. The result follows.

We see in particular for such representations the images of I are cyclic (from the knowledge of I_t) of order prime to p.

9.2.2 The θ_d is in the character group $\mathrm{Hom}(I, k^\times)$. For $\alpha \in (\mathbb{Q}/\mathbb{Z})'$, (where ' means those elements of order prime to p) we let, if $\alpha = a/d$, $(d, p) = 1$,

$$\gamma_\alpha = (\theta_d)^a$$

χ_α depends only on α. This gives

Proposition 15. (Serre [8] prop.5) The map $\alpha \mid \longrightarrow \chi_\alpha$ is an isomorphism from $(\mathbf{Q}/\mathbf{Z})'$ to $\mathrm{Hom}(I, k^\times)$.

Proof. This refers to the "finite" case as both of them are limit. Our construction of the maps is the same in that case.

The discussion helps us to compute the exact image of some characters.

9.3. Character of $\mathbb{Q}$ unramified outside p.

Let's consider a character Θ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in a finite field of characteristic p which is unramified outside p. Now because Θ inducse an isomorphism

$$\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{im}\,\Theta$$

for some finite extension K of $\mathbb{Q}$ which is certainly cyclotomic, one sees, e.g., by considering the discriminant that $K = \mathbb{Q}(\mu_n)$ with some root of unity μ_n of order p^n. But χ_p generates the character group of $\mathrm{Gal}(K/\mathbb{Q})$ so Θ is a power of χ_p : $\Theta = \chi_p^m$. cf. also lemma 1 of §2.1.

10. λ-adic representations. Refernce: Ribet [2]

In [2] Ribet has extended the theory of ℓ-adic representation to λ-adic representation, as already indicated by Serre. Let's recall some basic definitions.

10.1. The definition.

For a number field E, let λ be a prime ideal (or a finite place) of E and E_λ the completion of E at λ. A λ-adic representation of a field K is a continuous homomorphism

$$\pi_\lambda : \mathrm{Gal}(K_s/K) \longrightarrow \mathrm{Aut}(V)$$

where V is a finite dimensional vector space over E_λ.

So a λ-adic representation can naturally be considered as an ℓ-adic one; and conversely an ℓ-adic representation, by extension of scalar, can result in a λ-adic representation.

Example. For V a finitely generated module over $E_\ell = E \otimes \mathbb{Q}_\ell$, there is a canonical decomposition

$$V = \prod_{\lambda | \ell} V_\lambda \quad \text{according to} \quad E_\ell = \prod_{\lambda | \ell} E_\lambda$$

Therefore for each λ, V_λ is a finite dimensional vector space over E_λ (or equivalently

$$V_\lambda = V \otimes_{E_\ell} E_\lambda$$

where E_λ is E_ℓ-module by the projection $E_\ell \longrightarrow E_\lambda$) Then for an ℓ-adic representation $\pi_\ell : G \longrightarrow \mathrm{Aut}\ (V)$ by which G acts E_ℓ-linearly on V, we have the λ-adic representations, for each λ.

$$\pi_\lambda : G \longrightarrow \mathrm{Aut}\ (V_\lambda)$$

by projection (or scalar extension). One sees $\pi_\ell = \prod_{\lambda | \ell} \pi_\lambda$.

10.2. Basic questions.

All concepts and procedures in §2 can be similarly defined for λ-adic representations of number fields (e.g. "rational" is replaced by "E-rational"). We do not treat it here; but will use the notions freely.

10.3. The representation attached to a Serre's torus.

Note that our construction in §5 of the ξ_ℓ's with values in a Serre's torus S_m concerns only with K, the number field on which representations of its Galois group is being considered. Under this circumstance, when the representations ξ_ℓ's are constructed, if we consider the λ-adic represention of S_m instead of the ℓ-adic ones, we actually obtain λ-adic representations.

Exactly proceed in the same manner, these ℓ-adic representations still satisfy the basic properties, e.g. all those in §5.5 with suitable modification.

10.4. Local algebraicity.

We turn to the local algebraicity. With similar definitions, one has the similar properties. Ribet proves furthermore

Proposition 16. (Ribet [2] corol.1.5.2) For a λ-adic representation of a number field, the ℓ-adic local algebracity implies that of λ-adic one.

Similar facts as in §8 still hold. In prticular an analogue of thm.10 can be proved. As the second main theorem of Ribet [2], thm.13 has also been generalized to the λ-adic case.

10.5. Some related results. (Ribet [1] §1)

K is a number field here.

Proposition 17. (Ribet [3] thm.1.1) Suppose π is a λ-adic representation of K and π' is a λ'-adic representation of K compatible with π (implicitly we assume

both π and π' are rational). Soppose K is either $\mathbb{Q}$ or a compositum of quadratic extensions of $\mathbb{Q}$. If the semi-simplification of π is Abelian, so is that of π'.

Proof. We can consider only the semi-simplifications of π and π'. The assumption on K allows us to apply thm.11 to ensure these semi-simplifications are locally algebraic. The result then follows immediately from thm.10 and prop.1 (actually their λ-adic analogues, we abuse them).

Proposition 18. (Ribet [3] thm.1.2) Let (π_λ) be a system of strictly compatible 2-dimensional λ-adic representations of K. Assume for each finite extention L of K, each λ, the semi-simplification of the restriction $\mathrm{res}_L(\pi_\lambda)$ of π_λ is not Abelian. For each prime ℓ, let π_ℓ be the direct sum of the representations π_λ for $\lambda | \ell$; so π_ℓ is a continuous map:

$$\pi_\ell : G \longrightarrow \mathrm{Aut}_{E \otimes \mathbb{Q}_\ell} V ,$$

where V_ℓ is a free E_ℓ-module of rank 2. Suppose that there is a postive integer n such that for each ℓ $\det \cdot \pi_\ell = \chi_\ell^n$. Then for each ℓ, we have an inclusion

$$G_\ell \hat{=} \pi_\ell(G) \subseteq \{ u \in \mathrm{Aut}_{E_\ell} V \ : \det(u) \in \mathbb{Q}_\ell^\times \} \hat{=} B_\ell .$$

Furthermore, if G_ℓ is open in B_ℓ for one ℓ, G_ℓ is open in B_ℓ for all ℓ.

Part II The ℓ-adic representations attached to elliptic curves

1. Definition and basic facts.

1.1. Elliptic curves.

An elliptic curve E defined over a field K is a complete, irreducible, non-singular curve of genus 1 over K together with a K-rational point O; or, when an embedding in the projective space is chosen, by Riemann-Roch, E is a non-singular cubic curve:

$$(1) \qquad y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6 \qquad a_i \in K.$$

If $\mathrm{char}K \neq 2, 3$, this equation can be put into the Weierstrass form

$$y^2 = 4x^3-g_2x-g_3.$$

(see Gross [1] or Tate [2]) In this case let

$$j = g_2^3/(g_2^3-27g_3^2).$$

j is the modular invariant of the elliptic curve (cf. Part III § 1.2). $\Delta = g_2^3 - 27g_3^2$ is the discriminant. Two elliptic curves are isomorphic (or bi-regular equivalent) over $\overline{K}$ iff they have the same modular invariant.

Example. If charK = 0, then E can be viewed as an elliptic curve defined over $\mathbb{C}$. In this case, E is just, geometrically, a complex torus.

1.2. Division points of elliptic curves.

E has an Abelian group structure with zero element O which is K-rational. (see Shimura [1]) Let

$$E_n = \text{kernel of multiplication by } n$$

then one knows, if $(n, \text{charK}) = 1$, that

$$E_n \simeq (\mathbb{Z}/n\mathbb{Z})^2 .$$

We adopt the following notation:

$$E_\infty = \text{torsion part of } E = \cup E_n;$$
$$E_{l^\infty} = \cup E_{l^r} = \text{torsion of order } l^r$$
$$= l\text{-th primary part of } E_\infty.$$

Then

$$E_{l^\infty} \simeq (\mathbb{Q}_l/\mathbb{Z}_l)^2 \qquad \text{if } (l, \text{charK}) = 1;$$

$$E_\infty \simeq (\mathbb{Q}/\mathbb{Z})^2 \qquad \text{if} \quad \text{char}K = 0.$$

The decomposition

$$E_\infty = \prod_\ell E_{\ell^\infty}$$

corresponds to the canonical isomorphism

$$\mathbb{Q}/\mathbb{Z} = \prod_\ell (\mathbb{Q}_\ell/\mathbb{Z}_\ell).$$

1.3. The ℓ-adic representations attached to elliptic curves.

We assume that K is of characteristic 0. Then $G = \mathrm{Gal}(\overline{K}/K)$ acts on the division points of E and therefore induces

$$\phi_n : G \longrightarrow \mathrm{Aut}(E_n) \simeq GL(2, \mathbb{Z}/n\mathbb{Z})$$

for each n. Taking limit (equivalent to that G acts on E_∞) we have

$$\phi_\infty : G \longrightarrow \mathrm{Aut}(E_\infty) \simeq GL(2, \hat{\mathbb{Z}}) \quad (\simeq \prod_\ell GL(2, \mathbb{Z}_\ell))$$

Similarly

$$\phi_{\ell^\infty} : G \longrightarrow \mathrm{Aut}(E_{\ell^\infty}) \simeq GL(2, \mathbb{Z}_\ell).$$

All these maps are naturally compatible (through projection, reduction, etc.)

Remark The Tate module T_ℓ is defined by $T_\ell = \varprojlim E_{\ell^n}$ which is isomorphic to $(\mathbb{Z}_\ell)^2$. Let $V_\ell = T_\ell \otimes \mathbb{Q}_\ell$. The action of G on T_ℓ gives again

$$\rho_\ell : G \longrightarrow \mathrm{Aut}(T_\ell) \simeq GL(2,\mathbb{Z}_\ell).$$

Obvious $\rho_\ell = \phi_{\ell^\infty}$.

We can construct the cyclotomic character χ_ℓ of G by the action of G on the ℓ^n-roots of unity in K. (cf. Part I, §3). We have the following commutative diagram:

(2)
$$\begin{array}{ccc} G & \xrightarrow{\rho_\ell} & GL(2,\mathbb{Z}_\ell) \\ & {\scriptstyle \chi_\ell} \searrow \quad \swarrow {\scriptstyle \det} & \\ & \mathbb{Z}_\ell^\times & \end{array}$$

This diagram can be realized by Weil's pair $e(\ ,\ )$ (in fact, $\bigwedge^2 T_\ell(E) = T_\ell(\mu)$), cf. Shimura [1].)

Let $G_n^{\sim} = \mathrm{im}\,\phi_n$; $G_\ell = \mathrm{im}\,\phi_{\ell^\infty} = \mathrm{im}\,\rho_\ell$. The latter one is an ℓ-adic Lie group, being a closed subgroup of $GL(2,\mathbb{Z}_\ell)$. Let $\mathfrak{G}_\ell$ = the Lie algebra of G_ℓ. G_ℓ will be replaced by its open subgroups under scalar extensions of the base field of finite type over the field of definition; in particular $\mathfrak{G}_\ell$ is invariant under such scalar extensions. This fact holds for Abelian varieties (Serre [1]).

1.3.1 For an Abelian variety (cf. Mumford [1] chap.2) X

of dimension g defined over a field K, let the notations be just the correspponding ones to elliptic curves by replacing E by X (e.g., X_n = kernel of multiplication by n). One knows then

$$X_n \approx (\mathbb{Z}/n\mathbb{Z})^{2g} \qquad \text{if } (n, \text{char}K) = 1.$$

We have similarly the ℓ-adic representation (assume $(\ell, \text{char}K) = 1$):

$$\rho_\ell : \text{Gal}(\overline{K}/K) \longrightarrow \text{Aut}(T_\ell)$$

where T_ℓ is the Tate module (again $V_\ell = T_\ell \otimes \mathbb{Q}_\ell$). (see Shimura [1])

Let $R = \text{End}(X)$ and assume that all endomorphisms of X are defined over K. R acts on $T_\ell(X)$ and the action of G commutes with that of R. We have actually the representation

$$\rho_\ell : G \longrightarrow \text{Aut}_R(T_\ell).$$

Similarly in case that there is an injection

$$F \longrightarrow \text{End}_K(X) \otimes \mathbb{Q},$$

where F is a field of some degree d over $\mathbb{Q}$ (say at this time that X is of type F) V_ℓ is then an F hence $F_\ell = F \otimes \mathbb{Q}_\ell$ module, and G acts F_ℓ-linearly (obvious). From the example of §10.2 of Part I we have the corresponding λ-adic

representation associated to the Abelian variety X:

$$\rho_\lambda : G \longrightarrow \mathrm{Aut}_{F_\lambda}(V_\lambda)$$

where λ is a place of F. Then the basic fact is

Thoerem (Ribet [2] thm.2.1.1-2) V_ℓ is a free F_ℓ-module of rank $h = 2g/d$. The dimension of the λ-adic representations is independent of the prime λ. Moreover the system (ρ_λ) attached to X is strictly compatible F-rational with exceptional set contained in the set of places where X has bad reduction. (see §1.5 below)

Remark The basic relation $\det \cdot \rho_\ell = \chi_\ell$ still holds under the assumption that $(\mathrm{End}_K X) \otimes \mathbb{Q}$ contains a totally real number field of degree $d=g=\dim X$. (Ribet [2])

1.4. Complex multiplication.

One can see (cf. Shimura [1])

$\mathrm{End}(E) = \mathbb{Z}$ or an order in an imaginary quadratic extension of $\mathbb{Q}$.

In the latter situation, $\mathrm{End}(E)\otimes\mathbb{Q}$ is the quadratic field. We say then E has complex multiplication by this quadratic field. In the former situation, we say E does not have com-

plex multiplication.

If E has complex multiplication, its modular invariant j is an algebraic integer if E is defined over a number field K.

Remark We will use the abbreviation CM ad libitum for the term "complex multiplication" in any sense, while non CM for the situation without complex multiplication.

1.5. Good reduction.

Let v be a discrete valuation of a field K with ring A, maximal ideal m and residue field $k = A/m$ of characteristic $p(v)$. If the elliptic curve E has a defining equation in A with discriminant a v-unit, then modulo m (coordinatewise), we have an elliptic curve $\tilde{E}$ over k. j is now a v-integer. We say at this time that E has good reduction at v. Conversely when j is v-integer, E has good reduction in a finit extension (e.g. by adding a twelfth root of a prime element) of K. We say then E has potential good reduction at v. For places at which E does not have potential good reduction we say E has bad reduction there.

Now assume that K is a number field. First note that E has good reduction at almost all places. Let ℓ be given. If $p(v) \neq \ell$, the reduction map induces an isomorphism between the Tate's modules T_ℓ of the elliptic curve E and

its reduction $E_v^{\sim}$ at v. Therefore the action of G via ρ_ℓ coincides with that via $\rho_\ell^{\sim}$ for this v. And the Frobenius coincides with that, say F_v, of $E_v^{\sim}$ under the above identificaton of the Tate's modules. Hence

$$\det(F(v)_{\rho_\ell}) = \det(F_v); \quad \det(1-F(v)_{\rho_\ell}) = \det(1-F_v).$$

But on the other hand

$$\det(F_v) = Nv; \quad \det(1-F_v) = 1-\mathrm{Tr}(F_v)+Nv = A_v$$

where A_v is the number of k_v-points of $E_v^{\sim}$ (being the number of the fixed points of the Frobenius!). This is conjectured by E.Artin and is proved by Hasse. In particular, ρ_ℓ is unramified at v. The Neron-Ogg-Safarevic Criterion says (cf. Serre [6] IV) that if ρ_ℓ is unramified at v then E has good reduction at v. Note in particular the system so obtained is rational (in fact integral) strictly compatible with exceptional set contained in the set of places where E has bad reduction.

More general for an Abelian variety X defined over K, we can also define that X has good reduction at v if $X \simeq X_v \times K$ for some Abelian scheme X_v over the ring of v-integers. At this time the Neron-Ogg-Safarevic Criterion still holds: X has good reduction at v iff the Tate module (as Galois module) is unramified at v. For more detail see Serre & Tate [1].

1.6. Types.

We maintain the assumption of last subsection.

Consider the Tate module T_p of the reduction curve $E_v^{\sim}$ where $p(v) = p$. One knows either $T_p \simeq \mathbb{Z}_p$ or $T_p = 0$. We then call E to be of type I and II at v, respectively. Assume that the residue field k is finite. We have

Proposition 1. (Serre [2] Prop.1 of §1.3)

(a) If E is of type I, then for any n, $F(v)^n \neq$ hometheties where $F(v)$ is the Frobenius.

(b) If E is of type II, then $F(v)^4$ or $F(v)^6 =$ homothety.

Remark For an elliptic curve E defined over a field of char.$= p$, its height h is the integer h such that p^h is the inseparable degree of "multiplication by p". For an endomorphism α of E, α induces a homomorphism on the function field, $\alpha^* : K(E) \longrightarrow K(E)$. Then its separable and inseparable degrees are the counterparts of the field extension $K(E)/\alpha^*(K(E))$.

A formal group (of dimension 1) over a commuutative ring R is just a formal power series $F(X,Y)$ which gives a formal group law:

$$F(X, 0) = X, \quad F(0, Y) = Y$$

$$F(F(X, Y), Z) = F(X, F(Y, Z)).$$

This in fact supplies a group operation as one can always find "the inverse". For another formal group $G(X, Y)$ a homomorphsm $f: F \longrightarrow G$ is also a power series $f(X)$ such that

$$f(F(X, Y)) = G(f(X), f(Y)).$$

Its height for a given prime number p is the maximal integer h such that $f(X) = g(X^{p^h})$ for some g. (cf. Frohlich [1])

Under the new variables

$$z = -x/y, \quad w = -1/y, \quad \text{and so} \quad x = z/w, \quad y=-1/w$$

equation (1) for the elliptic curve E becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 \cdots\cdots.$$

If $P_3 = P_1 + P_2$, and $P_i = (z_i, w_i)$, then

$$z_3 = F(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 - \cdots\cdots$$

brings E a formal group structure. Now the facts are

(i) The height of E is equal to that when E is viewed as a formal group;

(ii) For an E defined over a number field with $p(v)=p$, $\tilde{E_v}$ reduction at v, the following are equivalent: (ii.1)

height = 1; (ii.2) $T_p \approx \mathbb{Z}_p$ (i.e. E is of type I at p). And the following are equivalent: (ii.1)' height = 2; (ii.2)' $T_p = 0$ (i.e. E is of type II at p).

1.7. Remark on CM.

If E has CM by L which is a quadratic extension of $\mathbb{Q}$, then $R = \mathrm{End}_{\bar{K}}(E)$ is an order in L, and naturally acts on V_ℓ, so does L. As R is defined over a finit extension of K, G has an open subgroup whose action on V_ℓ commutes with that of R hence the action of $\mathfrak{G}_\ell$ commutes with that of R, cf. §1.3. Since the commutating algebra of L in $gl(V_\ell)$ is $L_\ell = L \otimes \mathbb{Q}_\ell$, we see in particular $\mathfrak{G}_\ell$ is Abelian.

2. An overview.

2.0. General consideration.

When the ℓ-adic representation is constructed from an Abelian variety X, the fundamental problem is to determine its image. Our interest here is the case that the definition field of X is a number field.

Clearly the most complete knowledge will be that

about Φ_∞: $G \longrightarrow \mathrm{Aut}(X_\infty) \simeq GL(2g, \hat{\mathbb{Z}})$. Two questions of first consideration are the Lie algebra $\mathcal{G}_\ell$ and the Lie group G_ℓ. (They become equivalent under certain conditions, see Lemma 5 of §7.1.)

For the Lie algebra $\mathcal{G}_\ell$, it is expected that there is a reductive Lie algebra $\mathcal{G}$ over $\mathbb{Q}$ such that $\mathcal{G}_\ell = \mathcal{G} \otimes \mathbb{Q}_\ell$ (independent of ℓ). In view of our above consideration, as G commutes with some operators (e.g. elements in the field of complex multiplication), $\mathcal{G}_\ell \subseteq$ the commutant of these operators. $\mathcal{G}_\ell$ is also expected to be "as large as possible", namely, $\mathcal{G}_\ell$ is just the commutant of these obvious operators (on $T_\ell(X)$). This is exactly so for the cases discussed in this chapter. In the modular case (Chapter III) we would find some "extra twists" which leave difficulty (to determine them) and deter $\mathcal{G}_\ell$ from being equal to the expected obvious one. However the results still hold with $\mathcal{G}$ replaced by a suitably chosen Lie algebra.

Then G_ℓ, when the situation for $\mathcal{G}_\ell$ is well behaved, will be open in a unversally defined (rational) Lie group H_ℓ (cf. the results below) which is the largest one with Lie algebra $\mathcal{G}_\ell$. Then we expect $G_\ell = H_\ell$ at least for almost all ℓ. "Almost all ℓ" is always our aim. The known results for Abelian varieties are satisfatory. A technique for this can be stated as: always take the reduction to consider the modulo ℓ (a prime) case. This is based on thm.1A, 4A and prop.21 under the assumption that prop.20 (or an analogue one) holds. The applicability of the argument of prop.21 is worth noticing. With some elaborate group

theoretic analysis we are led to realize some special conditions (e.g. prop.19A (Ribet)). Note that in any cases the basic relation

$$\det \circ \rho_\ell = \chi_\ell$$

is required. Reduction seems to be the only known effective method for group level problem (cf. Serre [11])

The discussion will be similar for the modular case.

2.1. The Lie algebras.

This will cover the content of §3-4.

For the Lie algebras, as one of the main problems, first we will consider the local case following Serre. It was completed in his [2] and retreated in more detail in the Appendix of [6] IV. Technically speaking, two methods are used, namely irreducible theorems and some kinds of short exact sequences. Essentially, we have to understand, e.g., semi-simplicity of the representations from algebraic geometry.

Then we apply these results to the global case. They are more or less related to the careful analysis of the algebraic structures of $GL(V)$ and $gl(V)$ (as well as results on Abelian varieties and p-divisible groups, certainly). The CM case is determined in Serre [2] (thm.12). For the non CM case, in the same paper, incomplete results are ob-

tained (particularly verified for Tate's curve!). This case is determined in Serre [6] (thm.13), using a "new" technique i.e. the irreducible theorem (Lemma 3), as well the results for Abelian representations. (To attach an Abelian representation to a Serre's torus; this is also used in the proof of thm.22, cf. § 8) As interesting facts some density theorems (§ 6) are proved in Serre [2], (prop.17-19) they are used, latter in [8], in the proof of thm.22.

2.2. Isogenous theorem.

It indicates the strong connection between an elliptic curve and its Tate module. They are discussed in §5 but have no applications here. (cf. Remark in §3.2)

2.3. The Lie groups G_ℓ.

To determine the image of ρ_ℓ itself in a more explicite manner, e.g. thm.22, we have used prop.21 to indicate the various ways to obtain this (concentrating on non CM case) , cf. also INTRODUCTION of Serre [8] for more equivalent statements, based on one of which we have proved thm.27 for the non CM case. (cf. thm.25 for paralell of the CM case) In most cases, as mentioned before, reduction is the only way to work on the group level. These facts are treated in §7-8.

2.4. Generalizations.

In §9, we give some consideration about the "exceptional primes". We follow Serre to treat these facts. §10 is a slight generalization to the case of product of curves. The rest is devoted to the statements of the results about Abelian varieties with real and complex multiplication by Ribet [2] and Serre & Tate [1].

3. Local case.

To begin with, it is convenient to consider the local case first. In the sequal E denotes an elliptic curve defined over a field K with modular invariant j.

3.0. Notations.

Let K be a field with discrete valuation v, with the same notations as in the beginning of §1.5. Then we have two cases, $v(j) < 0$ and $v(j) \geqslant 0$.

3.1. Tate's curves.

In the former case (i.e., $v(j) < 0$) we have Tate's elliptic curves (cf. Robert [1]). The fact is that we completely understand the group structure, from which we obtain a

non-split short exact sequence of G-modules:

$$(3) \qquad 0 \longrightarrow V_\ell(\mu) \longrightarrow V_\ell(E) \longrightarrow \mathbb{Q}_\ell \dashrightarrow 0$$

where $V_\ell(\mu)$ is the cyclotomic representation space and $\mathbb{Q}_\ell$ is a trivial G-module, as follows. Let $q \in K^\times$ be such that $v(q) = -j$, then $E \approx E_q$ in a finite extension of K where E_q is the Tate elliptic curve determined by q (cf. Robert [1] or Lang [1]). Identify them. As $E(K) = K^\times/\Gamma$ where $\Gamma = q^{\mathbb{Z}}$, we have $E_n = \{ z : z^n \in \Gamma \}$. For $z \in E_{\ell^n}$ $z^{\ell^n} = q^c$ where c in $\mathbb{Z}/\ell^n\mathbb{Z}$ is uniquely determined by z. This gives a map $E_{\ell^n} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z}$. If μ_n is the group of the ℓ^n-th roots of unity then one sees easily that there is an exact sequence:

$$(3)' \qquad 0 \longrightarrow \mu_n \longrightarrow E_{\ell^n} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow 0.$$

Taking inversse limit with respect to n then tensoring by $\mathbb{Q}_\ell$ we have the above desired exact sequence, noticing the system (μ_n) is surjective.

Lemma 1. (Serre [6] IV Appendix) The exact sequence (3) does not split (as G-modules).

3.1.1 Remark There is higher dimensional analogue of Tate's elliptic curves, namely the parametrized Abelian varieties, due to Mumford. cf. a list of some facts in Ribet [2] III §2.

Again for these parametrized Abelian varieties associated to an admissible

$$q: M \longrightarrow \mathrm{Hom}(N, K^{\times})$$

where M and N are free Abelian groups of rank $d=\dim X$, we have a short exact sequence:

$$0 \longrightarrow \mathrm{Hom}(N, T_{\ell}(\mu)) \longrightarrow T_{\ell}(X) \longrightarrow M \otimes \mathbb{Z}_{\ell} \longrightarrow 0.$$

This exact sequence is functorial in X. It plays a similar role as (3) in Ribet [2].

Let i_{ℓ} denote the Lie algebra of the image of the inertia subgroup of G by ρ_{ℓ}. Then (for the notations, see §7.1, Part IV)

Proposition 2. (Serre [2] thm.3 of 2.4 or [6] thm. of IV A.1.3) Let $X = V_{\ell}(\mu)$. Assume that K is a local field. Then $\mathcal{G}_{\ell} = r_X$. $i_{\ell} = n_X$ if $\ell \neq p(v)$; $i_{\ell} = r_X$ if $\ell = p(v)$.

Proof. The action of $\mathcal{G}_{\ell}$ is clearly illustrated by the exact sequence. For i_{ℓ}, the trick is to replace K by its maximal unramified extension where $i_{\ell} = \mathcal{G}_{\ell}$. But the result about the exact sequence (3) still holds. We have seen that in order to determine the action of $\mathcal{G}_{\ell}$, what we need is the action of G on $V_{\ell}(\mu)$, which is well acquainted. We have

Proposition 3. (Serrs [6] Thm. of IV A.1.3) If k is algebraically closed then, $\mathcal{J}_\ell = n_x$ if $\ell \neq p(v)$; $\mathcal{J}_\ell = r_x$ if $\ell = p(v)$.

3.1.2 Recall

Proposition 4. Tate elliptic curve does not have CM. (cf. Robert [1] (3.16.), p.207)

Remark Tate elliptic curves are convenient test objects, and useful, cf. the result for parametrized Abelian varieties (Ribet [2]).

3.2. Good reduction.

In the second case (i.e., $v(j) \geqslant 0$), we have the concept of good reduction (up to a finite extension of the base field, cf. potential good reduction). It brings us unramifiedness (and, in global case, rationality). We discuss the cases $\ell \neq p(v)$ here and $\ell = p(v)$ in §3.3.

Proposition 5. (Serre [2] §2.2 or [6] IV A.1.2) $i_\ell = 0$. $\mathcal{J}_\ell$ is one dimensional.
as the Frobenius generates G topologically.

3.3. Good reduction: the crucial case $\ell = p(v)$.

When $\ell = p(v)$, it becomes a little bit more difficult because the reduction curve is degenerated. The fact is, our understanding of the situation in this case is essential for the determination of the image. The results here indeed supply more information. There are two types.

3.3.1 Type II: the reduction curve $E^{\sim}$ is of height 2, the result depends on an irreducibility theorem, saying that

Lemma 2. (Serre [10]) $\mathcal{G}_{\ell}$ acts irreducibly on V_{ℓ}.

Proposition 6. (Serre [2] thm.2 of 2.3 or [6] thm. of IV A.2.2) $\mathcal{G}_{\ell} = i_{\ell}$. They are equal to either $\mathrm{End}(V_{\ell})$ or a non-split Cartan subalgebra.
(cf. §4.2.3 below and the technique in prop.1 above)

3.3.2 Type I: the reduction curve $E^{\sim}$ is of height 1. Then as the Tate module $V_{\ell}(E^{\sim})$ of the reduction curve E is isomorphic to $\mathbb{Z}_{\ell}$, the reduction map

(4) $\quad V_{\ell}(E) \longrightarrow V_{\ell}(E^{\sim})$

has kernel X as a one-dimensional subspace of $V_{\ell}(E)$ stable under G (i.e., a G-submodule. Compare with (3).).

Proposition 7. (Serre [6] thm. of IV A.2.4) Suppose the residue field k is finite. Then the following are equivalent:

(a) E has CM over K;

(b) E has CM over a finite extension K'/K of K;

(c) There exists a one dimensional subspace D of $V_\ell(E)$ which is a G-supplementary of X;

(d) There exists a one dimensional subspace D of $V_\ell(E)$ which is $\mathcal{G}_\ell$-supplementary of X.

(This is based on more results on Abelian varieties) In particular, we have

Proposition 8. (Serre [2] thm.1 of §2.3 or [6] corol.1 of IV A.2.4) If E does not have CM then $\mathcal{G}_\ell = b_X$; $i_\ell = r_X$.

Proposition 9. (Serre [2] thm.1 of §2.3 or [6] corol.2 of IV A.2.4) If E has CM then $\mathcal{G}_\ell$ is the split Cartan subalgebra with respect to X and Y; and i_ℓ is the semi Cartan subalgebra trivial on Y, where

$$0 \longrightarrow X \longrightarrow V_\ell(E) \longrightarrow Y \longrightarrow 0, \text{ cf. prop.7.}$$

4. Global case.

We turn to the case that K is a number field. We find insterest of the group-theoretic analysis according to the local results. First we consider the images of the decomposition and the inertial subgroups, then we look more carefully into which kinds of groups can contain them. It can deduce some partial results.

Proposition 10. (Serre [2] prop.4 of §3.1) $\mathfrak{g}_\ell \neq$ Borel subalgebra of $\mathrm{End}(V_\ell)$.

Proof. Otherwise, one sees, if X being the unique G-stable line of V_ℓ, the Lie algebras of the images of any inertia subgroups $\subseteq r_x$ by checking case by case when places run, cf. local cases. Now G_ℓ is an open subgroup of the Borel subgroup with respect to X. The semi-simplification is given by two characters $\theta_1, \theta_2 : G \longrightarrow \mathbf{Z}_\ell^\times$. $\mathrm{im}\theta_i$ is a $\mathbb{Z}_\ell$-module of rank one (obvious). We have just seen the inertia subgroups have images in $\mathrm{im}\theta_1$ finite groups, so the Galois extension attached to $\mathrm{im}\theta_1/\mathrm{tor}(\mathrm{im}\theta_1) \simeq \mathbf{Z}_\ell$ is an infinite unramified Abelian extension with Galois group $\mathbb{Z}_\ell$, which is impossible. (reciprocity!)

Proposition 11. (Serre [2] prop.5 of §3.1) $\mathfrak{g}_\ell = \mathrm{End}(V_\ell)$ or $\mathfrak{g}_\ell =$ Cartan subalgebra of $\mathrm{End}(V_\ell)$.

Proof. If j is not an integer, we refer E to be a Tate's curve. At least $\mathfrak{g}_\ell \supseteq \mathrm{Lie}(\mathfrak{p}_\ell D(w)) = r_x$ with the nota-

tion in prop.2 for a place $w|\ell$ and $D(w)$ the decomposition subgroup. But $\mathfrak{g}_\ell \neq \mathrm{Lie}(D(w))$ according to Serre [1]. $\mathfrak{g}_\ell$ must contain the corresponding Borel subalgebra. But prop.10 shows $\mathfrak{g}_\ell$ is not this Borel subalgebra. Hence the result (thm.24A).

We consider now the case that j is an integer, but the rest are purely algebraic. For ℓ given, we choose a decomposition subgroup $D(w)$ where $w|\ell$ so as to apply prop.6, 8 or 9. We have in any cases $\mathfrak{g}_\ell \supseteq$ some Cartan subalgbra, or Borel subalgebra, or $\mathrm{gl}(V)$. Hence we can refer the proof to prop.24A & prop.10.

In two cases when E does or does not have CM the results appear quite different.

4.1. The CM case.

Assume that E has CM by F where F is an imaginary quadratic extension of $\mathbf{Q}$.

Theorem 12. (Serre [2] thm.5 of §3.3)

(a) $\mathfrak{g}_\ell$ = the Cartan subalgebra $F_\ell = F \otimes \mathbf{Q}_\ell$. It splits iff ℓ is decomposed in F;

(b) G_ℓ is Abelian if $K \supseteq F$; non-Abelian otherwise.

Proof. (a) follows easily from §1.7 and prop.11 (and the obvious fact that $\mathfrak{g}_\ell \neq$ homotheties). For (b), we refer to

the discussion in §1.7.

Remark The result here is related to the reciprocity law of Shimura about division points of elliptic curves. The complete result should be seen in thm.25.

4.2. non CM case.

The early work of Serre [2] about this case is incomplete. For example, using Tate's theory (cf. §3.1) he proves the expected result (thm.13) in case that j is not an integer. Also if one considers the local results and prop.11 above together with some group theory he can find that if thm.13 fails then $\mathfrak{g}_\ell$ has to be a non-split Cartan subalgebra. The results are obtained more or less by explicit group theoretic analysis. The fact of these two possibilities seems interesting since it depends on less properties.

4.2.1 In Serre [6] the problem of determining the Lie algebra was completely solved.

Theorem 13. (Serre [6] Thm. of IV §2.2) $\mathfrak{g}_\ell = \mathrm{End}(V_\ell)$.

This is based on the following irreducibility theorem:

Lemma 3. (Serre [6] thm. of IV §2.1) If E does not have CM, then

(a) V_ℓ is irreducible for all ℓ;

(b) E_ℓ is irreducible for almost all ℓ.

Proof. This follows from Safarevic's finiteness theorem:

Theorem The K-isomorphic classes of K-elliptic curves having good reduction outside a given finite set of places are finite

which refers to Siegel's theorem of the finiteness of solutions of the Diophantine equation

$$y^3 - 27x^2 = \Delta$$

in the ring O_S of S-integers in the number field K, where Δ is the discriminant of E, S is a finite set of places.

Remark (a) and (b) remain true when the definition field K is replaced by a finite extension as seen from the lemma itself.

Let's come back to thm.13. The hard part of the proof is to exclude the possibility that $\mathfrak{g}_\ell$ = non-split Cartan subalgebra, cf. §4.2.3 below.

When $\mathfrak{g}_\ell$ = non-split Cartan subalgebra, we may assume that G_ℓ is Abelian up to a finite extension. Then V_ℓ, for this ℓ, is rational, simple and Abelian. We have

Lemma 4. At this time (i.e., G_ℓ is Abelian) V_ℓ (or ρ_ℓ) is locally algebraic. (cf. Part I, §8)

4.2.2 A word digress. The proof of lemma 4 can be found in Serre [6] IV, in the proof of the same theorem in §2.2. The more general result for a λ-adic representation associsted to an Abelian variety, and the proof, using the concept of Hodge-Tate module, still hold. For this, see Ribet [2] thm.2.1.3.

Come back to our proof. Being so, ρ_ℓ comes from an algebraic representation of some S_m. So we have the system (W_ℓ) in the sense of §5.6, Part I. As (W_ℓ) is compatible with V_ℓ, so is with (V_ℓ). Hence they are the same. But infinitely many W_ℓ are diagonalized, this contradicts our irreducibility of the V_ℓ's.

4.2.3 Let's consider what would happen when an irreducible theorem holds. Recall that V is a 2-dimensional vector space.

The commutating algebra $C(\mathcal{G}_\ell)$ of $\mathcal{G}_\ell$ is now a skew field, which is a field by dimension reason. It is $\mathbb{Q}_\ell$ or a quadratic extension of $\mathbb{Q}_\ell$. In the former case $\mathcal{G}_\ell$ corresponds to $gl(V)$ or $sl(V)$. (Note that by (2) of §1.3 $G_\ell \subsetneq SL(V)$ provided K is not too large) For the second case, as $C(\mathcal{G}_\ell)$ acts irreducibly, $C(C(\mathcal{G}_\ell)) = C(\mathcal{G}_\ell)$. Hence $\mathcal{G}_\ell \subseteq C(\mathcal{G}_\ell)$ and consequently $\mathcal{G}_\ell = C(\mathcal{G}_\ell)$, i.e. $\mathcal{G}_\ell$ is a non-split Cartan subalgebra. In particular $\mathcal{G}_\ell$ is Abelian.

Conversely, once a Lie algebra is reducible, it is contained in a Borel subalgebra.

4.3. A remark.

Recall G_ℓ Abelian $\Longrightarrow$ $\mathfrak{G}_\ell$ Abelian $\Longrightarrow$ an open subgroup of G_ℓ Abelian. The last implication comes from the theory of Lie groups.

5. Isogeny and Tate module.

One knows that isogenous elliptic curves have isomorphic Tate modules. Here is the result about this fact under the assumption that j is not an integer. Recall that an isogeny of elliptic curves is a non-zero homomorphism.

5.1. Local case.

K is a local field of char= 0 here and the elliptic curves E and E' are defined over K.

Proposition 14. (Serre [6] Thm. of IV A.1.4) Assume $E = E_q$ and $E' = E_{q'}$ are two Tate elliptic curves. Then the following are equivalent:

(a) E and E' are K-isogenous;

(b) There exist integers $A, B > 1$ such that $q^A = q'^B$;

(c) $V_p(E)$ and $V_p(E')$ are isomorphic as $Gal(\bar{K}/K)$-modules where $p = char.k$ and k is the residue field.

Proof.

(b) ==> (a). This is because E_q is isogenous to E_{q^A} as the function field of the latter one is canonically identified as a subfield of that of the former one by Tate's theory.

(a) ==> (c). Obvious.

(c) ==> (b). For a given isogeny we have the associated map

$\Phi : T_p(E) \longrightarrow T_p(E')$,

because $\mathbb{Q}_p T_p(\mu)$ is the only G-line in $V_p(E)$ (and in $V_p(E')$; otherwise $V_p(E)$ splits, this contradicts our calculation about the Lie algebra in prop.2), maps $\mathbb{Q}_p \cdot T_p(\mu)$ to itself. Hence after multiplying Φ by a p-adic integer we can assume the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_p(\mu) & \longrightarrow & T_p(E) & \longrightarrow & \mathbb{Z}_p & \longrightarrow & 0 \\ & & \downarrow \tau & & \downarrow \Phi & & \downarrow \sigma & & \\ 0 & \longrightarrow & T_p(\mu) & \longrightarrow & T_p(E') & \longrightarrow & \mathbb{Z}_p & \longrightarrow & 0 \end{array}$$

where τ is the restriction of Φ to $T_p(\mu)$. So τ and σ are multiplication by p-adic integers s and t respectively. Let $x_n = d(1)$ where

$d: H^0(G, \mathbb{Z}/\mathfrak{p}^n\mathbb{Z}) \longrightarrow H(G, \mu_n)$

is the coboundary operator of the long exact sequence of G-modules of the exact sequence (3)' of §3.1. The naturality of the coboundary operator ensures that $x = (x_n) \in \varprojlim H^1(G, \mu_n)$. We have then

$$sx = tx'$$

if x' associated to E', from the long exact sequences. From Kummer theory we have

$$K^\times/K^{\times p^n} \simeq H^1(G, \mu_n)$$

which maps q to x_n. Therefore apply the map

$$\varprojlim H^1(G, \mu_n) = \varprojlim K^\times/K^{\times p^n} \longrightarrow \mathbb{Z}_p^\times$$

induced from the valuation map we have

$$sv(q) = tv(q').$$

We are to prove that $\alpha = q^{v(q')}/q'^{v(q)}$ is a root of unity. Consider α in

$$K^\times \longrightarrow \varprojlim K^\times/K^{\times p^n}$$

which is $v(q')x - v(q)x'$ in additive form and under previous identification. We see

$$t(v(q')x - v(q)x') = stv(q)x - tv(q)x' = 0$$

We are hereupon to consider the kernel of $K^{\times} \longrightarrow \varprojlim K^{\times}/K^{\times \mathfrak{p}^n}$. It is $\bigcap K^{\times \mathfrak{p}^n}$ which is finite from structure theorem (Weil [2] chap.3 prop.9). But a finite subgroup of the multiplicative group $K^{\times}$ is always consisting of roots of unity. That completes the proof.

5.2. Global case.

Assume that E and E' are elliptic curves defined over a number field K with modular invariants j and j'.

Proposition 15. (Serre [6] Thm. of IV 2.3) If $V_{\ell}(E) \simeq V_{\ell}(E')$ as G-modules and j is not an integer, then E and E' are K-isogenous.

Proof. $v(j) < 0$ for some place v then we can show $v(j') < 0$ also. So they are both Tate's curves, hence referred to prop.14 the local case. To conclue we need only a rationality argument.

The fact that $v(j) < 0$ implies $v(j') < 0$ follows from the Neron-Ogg-Safarevic Criterion. For, that $v(j') \geq 0$ means good reduction, but the property of having good reduction is invariant for isogeny.

Remark There is a place v at which j is not a v-integer. But possibly $p(v) \neq \ell$. The following proposition

of rationality (independent of ℓ) illustrates the trick of the proof.

Proposition 16. (Serre [6] Prop. of IV §2.3) The following are equivalent:

(a) The Galois modules $V_\ell(E)$ and $V_\ell(E')$ are isomorphic for all ℓ;

(b) The $V_\ell(E)$ and $V_\ell(E')$ are isomorphic for one ℓ;

(c) $Tr(F(v)) = Tr(F(v)')$ for all v where both curves have good reduction;

(d) $Tr(F(v)) = Tr(F(v)')$ for a set of places v of density 1.

Proof. This is almost apperant from the representation-theorectic aspect, noting that in any cases the Galois module V_ℓ is semi-simple (thm.12 & 13).

6. Density theorems.

From now on throughout the rest of this chapter K will denote a number field over which the curve E under discussion is defined, unless otherwise mentioned.

This section contains some theorems about density, which themselves seem interesting. They appear in Serre [2]. Let

$$\Sigma = \{ v : j \text{ is a } v\text{-integer } \& \ E \text{ is of type II at } v \}$$

Proposition 17. (Serre [2] prop.6 of §3.2)

(a) If $\mathfrak{g}_\ell$ = Cartan subalgebra and G_ℓ is non-commutative then $\tilde{\Sigma}$ is of density 1/2;

(b) In all the other cases $\tilde{\Sigma}$ is of density 0.

Proof. The idea is prop.1 and the equipartionness of the Frobenii according to Cebotarev's theorem by which we can compute the density using Haar measure. Construct

$$R_\ell = \{ u \in G_\ell : u^4 \text{ or } u^6 = \text{homothety} \}.$$

Then in view of prop.1, granting only those places having good reduction, we see

$$v \in \tilde{\Sigma} \quad \text{iff} \quad F(v)_{\rho_\ell} \subseteq R_\ell$$

where $F(v)_{\rho_\ell}$ is the Frobenius (class) at v with respect to ρ_ℓ.

Let μ be the normalized Haar measure on G_ℓ. Now R_ℓ is a subset of $GL(2,\mathbb{Z}_\ell)$ defined by some polynomials (i.e., u^4 or u^6 = homothety), so we can calculate the density of $\tilde{\Sigma}$ by computing the measure of the interier of R_ℓ. The rest refers to a discussion of the possible situation, in any cases we know the structure of the images (as they are in $GL(2)$) well. For example if H is the maximal Lie group with Lie algebra $\mathfrak{g}_\ell$, then $R_\ell = G_\ell \setminus G_\ell \cap H$. It is just the coset of $G_\ell \cap H$ in G_ℓ (index 2). This fact can be perceived from the split case.

We have separately

Proposition 18. (Serre [2] thm.5 of §3.3) With the notation as in thm.12, we have

(a) $v \in \sum^{\sim}$ iff $p(v)$ is not decomposd in F;

(b) $\sum^{\sim}$ is of density 0 if $F \subseteq K$; 1/2 otherwise.

Proof. (a) follows easily from prop.6, 9 and thm.12.

Proposition 19. (Serre [2] thm.6 of §3.4) Assume E does not have CM then $\sum^{\sim}$ is of density 0.

7. Variation of ℓ.

We have seen that G_ℓ is open in $GL(2,\mathbf{Z}_\ell)$ (non CM case) and in R_ℓ (CM case, for R, see §7.2 below). The problem is to determine G_ℓ for all ℓ in a more explicit form. In our case, it had been conjectured that G_ℓ should be $GL(2,\mathbb{Z}_\ell)$ (non CM case) and R_ℓ (CM case) at least for almost all ℓ. This will be proved to be the case. One can also say if he likes, therefore, that the image of the ℓ-adic representation is independent of ℓ as ℓ varies.

Proposition 20. (Serre [6] Lemma of IV §3.1)

(a) $\mathrm{im}(G \longrightarrow \prod_\ell \mathrm{Aut}(T_\ell) \xrightarrow{\det} \prod_\ell \mathbb{Z}_\ell^\times)$ is open in $\prod_\ell \mathbb{Z}_\ell^\times$;

(b) For almost all ℓ, $\det(G_\ell) = \mathbb{Z}_\ell^\times$ and $\det(G_\ell) = \mathbb{F}_\ell^\times$.

Proof. This is in fact part of the reciprocity for $\mathbb{Q}$, cf. (a) §3 of chapter I, as well (2) of §1.3.

7.1. The non CM case.

Proposition 21. (Serre [6] Prop. of IV 3.1) The following are equivalent:

(a) $\operatorname{im}\phi_\infty$ is open in $\prod \mathrm{GL}(V_\ell)$;

(b) For almost all ℓ, $G_\ell = \mathrm{Aut}(T_\ell)$;

(c) For almost all ℓ, $\phi_\ell(G) = \mathrm{Aut}(E_\ell)$;

(d) $G_\ell^\sim$ contains $\mathrm{SL}(E_\ell)$ for almost all ℓ.

Only (d) ==> (a) is not obvious; but the proof are much group theoretic. It is thm.2A. We rewrite it here.

Lemma 5. (Serre [6], Main Lemma of IV §3.1) Let G be a closed subgroup of $\prod \mathrm{GL}(2,\mathbb{Z}_\ell)$ and G_ℓ and $G_\ell^\sim$ are its images in $\mathrm{GL}(2,\mathbb{Z}_\ell)$ and $\mathrm{GL}(2,\mathbb{F}_\ell)$, respectively. Assume

(a) G_ℓ is open in $\mathrm{GL}(2,\mathbb{Z}_\ell)$ for all ℓ;

(b) $\operatorname{im}(G \longrightarrow \prod \mathrm{GL}(2,\mathbb{Z}_\ell) \xrightarrow{\det} \prod \mathbb{Z}_\ell^\times)$ is open;

(c) $G_\ell^\sim$ contains $\mathrm{SL}(2,\mathbb{F}_\ell)$ for almost all ℓ.

Then G is open in $\prod \mathrm{GL}(2,\mathbb{Z}_\ell)$.

Remark. We will prove one of the other conditions in prop.21

so as to show (a) is true (mostly (c) and (d) as emphasized in §2, by reduction mod $\mathfrak{l}$). This proposition has various generalizations which lead to a method to solve the problem of the determination of all G_ℓ simultaneously.

If the modular invariant j of the elliptic curve is not an integer then we can apply Tate's theory to give a relatively easy proof that the conditions of prop.21 are satisfied. In fact

Lemma 6. (Serre [6] IV §3.2 lemma 1) If j is not an integer then $G_\mathfrak{l}^{\sim}$ contains a transvection if $\ell \nmid v(j)$ for a a place v such that $v(j) < 0$.

Then the irreducible theorem, Lemma 3, shows that the reduction $G_\ell^{\sim}$ will at least contain, e.g.

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

hence contain $SL(2,\mathbb{F}_\ell)$.

Actually

Theorem 22. (Serre [8] Thm.2 of 4.2) If E does not have CM, then the equivalent conditions in prop.21 are satisfied (by proving (c)).

This is the major result of Serre [8]; for the

proof, cf. §8 below.

7.1.1 We show firstly some corollaries of thm.22. Let K_c = K(roots of unity).

Proposition 23. (Serre [8] §4.4 corol.2) The image of $\mathrm{Gal}(\overline{K}/K_c)$ by Φ_∞ is an open subgroup in $\prod \mathrm{SL}(T_\ell)$.

Proof. Refer to (1) of § 1.3 and prop.21, as one sees, by the definition of χ_ℓ,

$$\mathrm{Gal}(\overline{K}/K_c) = \bigcap \ker \chi_\ell .$$

So $\Phi_\infty(\mathrm{Gal}(\overline{K}/K_c)) = \Phi_\infty(G) \cap \prod \mathrm{SL}(T_\ell)$.

For $v \in \sum$, let $w|v$ be an extension of v to $\overline{K}/K$, $I(w)$ be the inertia group and J_v be the smallest closed normal subgrooup containing $I(w)$; J_v is independent of the choice of w.

Proposition 24. (Serre [8] §4.4 thm.4) $\Phi_\infty(J_v)$ is equal to the $p(v)$-th factor $\mathrm{GL}(T_{p(v)})$ of $\prod \mathrm{GL}(T_\ell)$ for almost all v.

The more elaborate version is

Proposition 24'. Put $\ell = p(v)$. Suppose $\ell \geq 5$, and that $\phi_\ell : G \longrightarrow \mathrm{Aut}(E_\ell)$ is surjective, and that E has good reduction at v, v is unramified over $\mathbb{Q}$. Being so, $\phi_\ell(J_v) = GL(T_{p(v)})$.

Proof. $I(w)$ acts trivially on $T_{\ell'}$ at each $\ell' \neq \ell$ and at each of the places v at which E has good reduction. So does J_v by contiuity. This means we have the inclusion

$$H \overset{\sim}{=} \phi_\infty(J_v) \subseteq GL(T_\ell) \subseteq \prod GL(T_{\ell'}).$$

Consider the reduction $H^\sim$ of H on $\mathrm{Aut}(E_\ell) = \mathrm{Aut}(T_\ell/\ell T_\ell)$. The results (a) and (b) §8.1 apply to show that $H^\sim$ contains a non-split Cartan subgroup or a semi-split Cartan subgroup. Apply our lifting property thm.4A to the commutator subgroup H' of H we see $H' = SL(T_\ell)$ (thm.12A). On the other hand as v is unramified $\lambda_\ell(I(w)) = \mathbb{Z}_\ell^\times$. It means the same as that the map

$$\det : H \subseteq GL(T_\ell) \longrightarrow \mathbb{Z}_\ell^\times$$

is surjective. The result follows.

7.2. The CM case.

Now consider the case that E has CM. Assume that $R = \mathrm{End}_K(E) \neq \mathbb{Z}$ with field of fractions F which is an imaginary quadratic extension of $\mathbb{Q}$. One has a natural embedding $F \longrightarrow K$ (if all endomorphisms of E are defined over K. cf. Serre [8] §4.5).

For each λ let $R_\lambda = R \otimes \mathbb{Z}_\lambda$, $F_\lambda = F \otimes \mathbb{Q}_\lambda$. Then the Tate module T_λ is a free R_λ-module of rank 1, and V_λ is also a free F_λ-module of rank 1. The action by

$$\rho_\lambda : G \longrightarrow GL(T_\lambda)$$

commutes with that of the elements of R because all elements of R are defined over K. Hence the image G_λ is contained in $R_\lambda^\times$ (cf. §4.2.3). (Note that means the same as a homomorphism

$$\psi_\lambda : I \longrightarrow R_\lambda^\times$$

where I is the idele group of K) Being so,

Lemma 7. (Serre & Tate [1], thm.10) There exists one and only one continuous homomorphism

$$\xi : I \longrightarrow F^\times$$

such that $\xi(x) = N_{K/\mathbb{Q}}(x)$ if $x \in K^\times$ & $\psi_\lambda(a) = \xi(a) N_{K_\mathfrak{p}/\mathbb{Q}_\lambda}(a_\lambda^{-1})$ (where the norm is automatically extended to I).

Theorem 25. (Serre & Tate [1], thm.11, Serre [8] §4.5 thm.5) The image $\phi_\infty(G)$ in $\prod R_\lambda^\times$ is an open subgroup.

Proof. This is a consequence of Lemma 7, as one notices that N is an open map even though viewed as one on I after taking product, and that ξ is locally trivial.

8. The proof of thm.22: non CM case.

If there are infinitely many prime numbers ℓ such that $\Phi_\ell(G) \neq \mathrm{Aut}(E_\ell)$, then we show that E will admit CM.

To avoid digress, let's first mention some facts. By careful considering of the

(a) image of the "tame" inertias, cf. Part I, §9.2;

(b) subgroups and their relationship in $GL(2,\mathbb{F}_\ell)$, cf. Part IV,

we are led to, then, two possibilities:

(i) $\Phi_\ell(G)$ is contained in a Borel subgroup, or in a Cartan subgroup;

(ii) $\Phi_\ell(G)$ is contained in the normalizer N of a Cartan subgroup C, but not in C.

In case (ii) we deduce that each quadratic extension K_ℓ determined by $\ker(G \longrightarrow N/C = \{\pm 1\})$ of K is in fact unramified. Therefore we can find one K' independent of infinitely many ℓ. In K' all Frobenii corresponding to non-decomposed places v have trace 0. In fact they have image -1 under $G \longrightarrow \{\pm 1\}$, cf. §4.5 of chapter IV. This implies the reduction there is of height 2, cf. prop.1. But we have calculated the density of the set of non-decomposed places (prop.17), which is equal to 0 since E has no CM, while on the other hand one sees directly from Cebotarev's Density Theorem that this set is of density 1/2!

In case (i), if one considers the semi-simplification, he obtains infinitely many Abelian ℓ-adic representations which are rational. They can be lifted to one by a lifting theorem of Serre (Part I thm.13) infinitely many times, by carefully considering the characters of G with values in k^* (cf. Part I, § 9 and §8.1 below. See also (*) in thm.13, Part I.). The lifting is still Abelian, but that is impossible in the case that E does not have CM!

8.1. Preliminary results.

Now we are going to see how (1) and (2) above are derived. Let the notations be as in §1.5 but charK = 0. Let $e = v(p)$. Recall that I_p is the Galois group of tamely ramified extension and I_t the tame inertia, and I the inertia subgroup.

First we have the fact that the map

$$\det \Phi_p = \chi_p^{\sim} : G \longrightarrow \mathbb{F}_p^{\times} ,$$

where $\chi_p^{\sim}$ is the mod p reduction of the cyclotomic character, is in fact (cf. Serre [8] prop.8) $\vartheta_{\tau_{-1}}$, here for the notation ϑ_A, cf. Part I § 9.2. Now we can assume that equation (1) of §1.1. has coefficients $a_i \in A$. Then we have the following cases: (Serre [8] §1.11)

(a) The Tate module T_p of the reduction curve at p is

isomorphic to $\mathbb{Z}_p$. Then similar to prop.9 of §3.6 we have

$$0 \longrightarrow X_p \longrightarrow E_p \longrightarrow \tilde{E_p} \longrightarrow 0.$$

So the image of G (respectively, I_p) by ϕ_p in $\mathrm{Aut}(E_p) = \mathrm{GL}(2, \mathbb{F}_p)$ is contained in the Borel subgroup

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \quad \left(\text{resp. } \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right)$$

And I_t acts on X_p and $\tilde{E_p}$, respectively, by θ_{p-1}^e and 1. Moreover if $e = 1$ we have two cases: (i) If I_p acts trivially on E_p then the image of I is cyclic of order $p-1$; (ii) If I_p acts non-trivially on E_p then the image of I_t is of order $p(p-1)$. They are represented respectively by the matrices of the form

$$\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

(b) The Tate module T_p of the reduction curve is 0. Then we have seen by $(x, y) \longmapsto t=x/y$ that

$$F(t, t') = t+t'+a_1tt'-a_2(t\,t'+tt')+\cdots$$

induces a formal group law F with $a_i \in A$ (see §1.6). Under this identification, F is of height 2. Furthermore by a result on formal group (Serre [6] prop.9) we have, if $e=1$, that: (i) The image of I in $\mathrm{GL}(E_p)$ is a cyclic group C of order p^2-1 (non-split Cartan subgroup); (ii) The image of G in $\mathrm{GL}(E_p)$ is C or the normalizer N of C depending on

that k contains $\mathbb{F}_{p^2}$ or not.

(c) The last case is that having bad reduction. By Tate's theory, the discussion in §3.2 is still available. So similar results remain true. In more detail, we have if $e = 1$ then (i) If I_p acts trivially on E_p, then the image of I_t in $GL(E_p)$ is cyclic of order $p-1$; (ii) If I_p acts non-trivially on E_p then the image of I_t is represented by the matrices of the form

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

This can be done because we know the exact characters by which the inertias act on E_p. Therefore we have in all cases that conditions of thm.11A are satisfied. This gives (i) and (ii) of §8.0.

9. Elliptic curves over $\mathbb{Q}$ (non CM case).

Assume E does not have CM in this section. Then our result can be stated as "for almost all λ, $G_\lambda^{\sim} = \mathrm{im}(\phi_\lambda) = GL(2,\mathbf{F}_\lambda)$", i.e., there only finitely many primes λ such that $\mathrm{im}(\phi_\lambda) \neq GL(2,\mathbb{F}_\lambda)$. In fact, thm.22 is equivalent to

Theorem 22'. The indices of $G_n^{\sim}$ in $GL(E_n)$ are bounded by an integer independent of n.

Those primes (at which Φ_ℓ is not surjective) are called exceptional primes. It is interesting to determine all exceptional primes. The usual method is to find an upper bound of the exceptional primes.

9.1. Exceptional primes.

We consentrate on those elliptic curves E defined over $\mathbb{Q}$ in the whole §9. Let S be the set of primes at which E has bad reduction.

Let (cf. §1.5) t_p = trace of the Frobenius of the reduction curve $\tilde{E_p}$ at p if $p \notin S$. Then we rewrite

$$t_p = 1 + p - A_p$$
$$\mathrm{Tr}(f_p) \equiv t_p \pmod{\ell}$$
$$\det(f_p) \equiv p \pmod{\ell}$$

where A_p is the number of $\mathbb{F}_p$-points of $\tilde{E_p}$ and f_p is the Frobenius, $\mathbb{F}_p$ the field of p elements. The following proposition indicates when $\Phi_\ell(G) \neq \mathrm{Aut}(E_\ell)$.

Proposition 26. (Serre [8] §5.4 prop.21) Assume that E is semi-stable and

(a) $\Phi_\ell(G) \neq \mathrm{Aut}(E_\ell)$;

(b) $\ell \neq 2, 3, 5$; or ℓ does not divide $v_p(j)$ for all $p \in S$.

Then

(i) $\Phi_\ell(G)$ is contained in a Borel subgroup of $\mathrm{Aut}(E_\ell)$;

(ii) The G-module E_ℓ has a Jordan-Holder composition series with quotients isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ.

(iii) We have $t_p \equiv 1+p \pmod{\ell}$ for all $p \in \Sigma \setminus S$.

Proof.

(i) In case $\ell \nmid v_p(j)$ for all $p \in S$, Lemma 7 of §7.1 is valid. Then we can apply thm.6A to reach the destination. In case $\ell \geq 7$, but G_ℓ is not contained in any Borel subgroups, then according to §8 we see $\Phi_\ell(G)$ will contain either a non-split or a semi-split Cartan subgroup. Then thm.11A applies to show there 3 possibilities for $\Phi_\ell(G)$, as shown there. They are all impossible.

(ii) We omit the proof.

(iii) Let the notations be just as in the beginning of this section. $p \neq \ell$. Then

$$t_p \equiv \mathrm{Tr}(f_p) \equiv \alpha' + \alpha'' \pmod{\ell}$$

where α' and α'' are the eigenvalues of the Frobenius at p. Because of (ii), we have thus $\{\alpha', \alpha''\} = \{1, p\}$. Hence our assertion for $p \neq \ell$.

We have consequently the following interesting corollary, which indicates one way to effectively calculate an upper boound of the exceptional primes. (cf. also Serre [8] §5.6 prop.24)

Theorem 27. (Serre [8] §5.4 corol.1) Suppose that E is semi-stable. Assume p is the smallest prime number on

which E has good reduction. Then $\phi_\ell(G) = \mathrm{Aut}(E_\ell)$ for all $\ell > (p^{\frac{1}{2}} + 1)^2$.

Proof. Assume the contaray. $p \geq 2$. Thereforre $\ell > 5$. Our previous theorem shows A_p is divisible by ℓ. So

$$A_p \geq \ell > 1 + p + 2p^{1/2}$$
$$A_p = 1 + p - t_p.$$

Therefore $t_p < -2p^{1/2}$. This contradicts the Riemann Hypothesis for $E_p^{\sim}$ (Weil [4] p.70 corol.3).

9.2. The image of ϕ_∞.

The extreme case $\phi_\infty(G) = \prod \mathrm{GL}(2,\mathbb{Z}_\ell)$ in this case (i.e., elliptic curves over $\mathbb{Q}$) will never be true.

Proposition 28. (Serre [8] §5.5 prop.22) For any elliptic curve E, the image of

$$\phi_\infty : G \longrightarrow \mathrm{Aut}(E_\infty) \simeq \prod \mathrm{GL}(2,\mathbb{Z}_\ell)$$

is always contained in a subgroup of $\mathrm{Aut}(E_\infty)$ of index 2.

Proof. For each $a \in \mathrm{Aut}(E_\infty)$ let $a_n^{\sim}$ be its "mod n reduction" in $\mathrm{Aut}(E_n)$. As $\mathrm{Aut}(E_2) \simeq S_3$ (see §5.3 loc. cit.), if we write ε for the signature $S_3 \longrightarrow \{\pm 1\}$ we have

$$\eta_A : G \longrightarrow \{\pm 1\}$$

by $\eta_A(s) = \varepsilon(\phi_\ell(s))$. The quadratic extension determined by

is in fact $\mathbb{Q}(\sqrt{\Delta})$ where Δ is the discriminant of E. Embed $\mathbb{Q}(\sqrt{\Delta})$ in a cyclotomic field $\mathbb{Q}(\mu_m)$ we can rewrite χ_Δ as the composition

$$G \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\alpha_\Delta} \{\pm 1\}$$

and we have the formula

$$\xi(\phi_\ell(s)) = \alpha_\Delta(\det(\phi_m(s)) \qquad \text{for} \quad s \in G.$$

Then it is obvious that

$$\phi_\infty(G) \subseteq H_\Delta \triangleq \{ a \in \mathrm{Aut}(E_\infty) : \xi(a_\ell) = \alpha_\Delta(\det a_\ell) \}.$$

H_Δ is of index 2 in $\mathrm{Aut}(E_\infty)$.

10. Product of two elliptic curves.

10.1. Notations.

Let E, E' be two elliptic curves, with the usual notations apperaing before. We will use the $'$ to denote the counterparts of E'. We assume that both E and E' do not have CM.

10.2. The representation $\bar{\phi}_\ell$

Two maps ϕ_n and ϕ'_n give the product map

$$\tilde{\Phi}_n : G \longrightarrow \mathrm{Aut}(E_n)\times\mathrm{Aut}(E'_n).$$

Let

$$A_n = \{ (u, u') \in \mathrm{Aut}(E_n)\times\mathrm{Aut}(E'_n) : \det(u) = \det(u') \}$$

then $\mathrm{im}\,\tilde{\Phi}_n \subseteq A_n$. Taking limit with respect to n we have

$$\tilde{\Phi}_\infty : G \longrightarrow A_\infty = \varprojlim A_n.$$

$A_\infty \subsetneq \mathrm{Aut}(E_\infty)\times\mathrm{Aut}(E'_\infty)$ is of the form

$$\prod A_\ell$$

where $A_\ell \subsetneq GL(T_\ell)\times GL(T'_\ell)$ consisting of those elements (u, u') such that $\det(u) = \det(u')$ $(\in \mathbb{Z}_\ell^\times)$.

Theorem 29. (Serre [8] §6.1 thm.6) Assume

(a) E and E' do not have complex multiplication;

(b) Two systems (ρ_ℓ) and (ρ'_ℓ) of ℓ-adic representations do not become isomorphic even on any open subgroup of G.

Then the image $\tilde{\Phi}_\infty(G)$ is open in A_∞.

Remark An analogue of prop.23 holds.

10.3. The proof of thm.29.

It is a typical applying of some algebraic facts; its idea has imitation in other situation. We will draw a sketch in what is to follow.

Step 1. $\operatorname{im}\bar{\Phi}_{\ell^\infty}$ is open in A_{ℓ^∞}, for each ℓ.
Transfer to considering the Lie algebra. This is sufficient. Let

$$\mathfrak{h}_\ell = \text{Lie algebra of } A_{\ell^\infty}$$
$$= \{ (u, u') \in \operatorname{End}(V_\ell)\operatorname{End}(V'_\ell) : \operatorname{Tr}(u)=\operatorname{Tr}(u') \}$$

Then $\mathfrak{G}_\ell \subseteq \mathfrak{h}_\ell$. The assumption guarantees that the projections from $\mathfrak{G}_\ell$ to each factor of the product $\operatorname{End}(V_\ell)\times\operatorname{End}(V'_\ell)$ are surjective. Then the "Goursat's lemma" (cf. thm.19A) shows if $\mathfrak{G}_\ell \neq \mathfrak{h}_\ell$, $\mathfrak{G}_\ell$ is the graph of an isomorphism from $\operatorname{End}(V_\ell)$ to $\operatorname{End}(V'_\ell)$. This isomorphism induces an isomorphism between the V's as $\mathfrak{G}$-modules. That contradicts (b).

Step 2. Consider the reduction. In view of the lifting theorem.4A, this is sufficient. We claim that if ϕ_ℓ and ϕ'_ℓ are surjective but $\bar{\Phi}_\ell$ not, then there exist

$$\varepsilon_\ell : G \longrightarrow \{\pm 1\} \quad \text{and} \quad f : E_\ell \longrightarrow E'_\ell$$

such that f is an isomorphism and

$$f \cdot \phi_\ell(s) = \xi_\ell(s)\, \phi'_\ell(s) \cdot f \qquad \text{for any } s \in G$$

ξ_ℓ is unramified at all thoes places which are unramified over $\mathbb{Q}$ and where E and E' have good reduction. (cf. thm.22A)
This is again the Goursat' lemma. The proof involves a more careful group-structural analysis for the choice of ξ_ℓ.

Step 3. For almost all ℓ, $\bar{\Phi}_\ell(G) = A_\ell$.
If not, for infinitely many primes ℓ, $\bar{\Phi}_\ell(G) \neq A_\ell$. Denote by L the set of primes ℓ such that $\bar{\Phi}_\ell(G) \neq A_\ell$, $\ell \geq 5$ and both ϕ_ℓ and ϕ'_ℓ are surjective. Let ξ_ℓ be as in step 2. We can assume furthermore that the ξ_ℓ are unramified at almost all places of K, independent of ℓ by step 2. Hence there are in fact finitely many ξ_ℓ (because the ξ_ℓ's value in $\{\pm 1\}$!). Now replace L if necessary we assume all ξ_ℓ are the same. Then E_ℓ and E'_ℓ become G'-isomorphic by step 2 if $G' = \ker\xi$. Let K'/K correspond to ξ. The proof of the Lifting Theorem in Part I now applies. At each place w of K', at which E and E' have good reduction we have

$$\mathrm{Tr}(F(w)) \equiv \mathrm{Tr}(F(w')) \pmod{\ell}$$

for $\ell \notin L$. The infinit ness of L implies that $Tr(F(w)) = Tr(F(w)')$. Therefore E and E' will be isomorphic over K', impossible!

Step 4. For almost all ℓ, $\Phi_\infty(J_v)$ is the ℓ-th factor A_{ℓ^∞} of A_∞ where $v|\ell$. (See §9.2 for the notations.) This again the Goursat's lemma.

Step 5. Complete, because the argument of lemma 5 of §7.1 is applicable (This shows why step 4. is necessary).

10.4. A remark.

This is the easiest generalization. The result and the proof here can be generalized to the case of the product of finitely many elliptic curves under the same assumption, like that Ribet has done for modular forms, cf. Part III §4.4.

11. Abelian varieties with real multiplication.

In [2], Ribet has generalized thm.13 to the case of an Abelian variety X of type E where E is a totally real number field of degree d=dimX. The group theoretic aspect related to that of Serre is, even though we are considering an ℓ-adic representation

$$\rho_\ell : G \longrightarrow GL(2d, \mathbb{Q}_\ell)$$

of degree 2d, by means of §1.3.1, we have actually:

$$\rho_\ell : G \longrightarrow \mathrm{Aut}_{E_\ell}(V_\ell)$$

where $\mathrm{Aut}_{E_\ell}(V_\ell) = GL(2, E_\ell)$ if $[E:\mathbb{Q}] = g!$

In the sequal of this section, we assume that X is an Abelian variety defined over K such that

(RM)
(1) All endomorphsms of X are defined over K;
(2) $\mathrm{End}(X)\otimes\mathbb{Q} = E$ is a totally real number field of degree $d = \dim X$ and
(3) X does not everywhere have potential good reduction.

11.1. A discussion on the Lie algebras.

In Ribet [2] there is a clear discussion about the Lie algebras, which is in fact a generalization of the idea of Serre in §12.3. This is helpful.

Fix a rational prime ℓ. The assumption is the same as in the first paragraph of this section, see also §1.5.1. In fact we need only (Ribet [2] §4 of Part IV):

(i) If $\lambda | \ell$ then ρ_λ does not have an Abelian semi-simplification even on any open subgroup of G;
(ii) $\det \rho_\ell = \chi_\ell$ (or more general χ_ℓ^k for some k).

Please notice that (i) is similar to Lemma 3 (see the Remark after Lemma 3). These two conditions will be satisfied under the assumption (RM). Let

$$\mathfrak{h}_\lambda = \{ u \in \mathrm{End}_{E_\lambda} V_\lambda : \mathrm{tr}(u) \in \mathbb{Q}_\ell \} .$$

(ii) implies immediately that $\mathfrak{g}_\lambda \subseteq \mathfrak{h}_\lambda$. Our question is that when the equality holds. Obviously this is so if their dimension are equal. But dimension is invariant under scalar extension. So let "-" denote the extension $\otimes \overline{\mathbb{Q}}_\ell$. First keep in mind that the restriction of $\mathfrak{g}_\lambda$ on any open subgroup of G acts irreducibly on V_λ because of (i). For any finite extension L/K, let $G_L = \mathrm{Gal}(\overline{K}/L)$. Convince that the results below are true for any L we thus disregard the function of L as subscript.

The discussion in §4.2.3 shows:

(a) $\mathrm{End}_{E_\lambda, G} V_\lambda = E_\lambda$ for all $\lambda | \ell$ and hence $\mathrm{End}_{E, G} V_\ell = E_\ell$

and by scalar extension

(a)' $\mathrm{End}_{\overline{E}_\ell, G} \overline{V}_\ell = \overline{E}_\ell$.

Let $\Gamma = \{ \sigma : E \longrightarrow \overline{\mathbb{Q}} \}$. Then we have a decomposition:

$$\overline{V} \quad (= V \otimes_{E_\ell} \overline{\mathbb{Q}_\ell}) = \coprod_{\Gamma} V_\sigma$$

as $\overline{E}_\ell[G] = E \otimes \overline{\mathbb{Q}}_\ell[G]$ -modules where $V_\sigma = \overline{V} \otimes_{E_\ell} \overline{\mathbb{Q}}_\ell$. The decom-

position actually comes from

$$\overline{E}_\ell \ (= E_\ell \otimes \overline{\mathbb{Q}}_\ell \ = E \otimes \overline{\mathbb{Q}}_\ell \ ) = \prod_{\overline{\Gamma}} \mathbb{Q}_\sigma$$

We see whereby V_σ is of 2-dimension over $\overline{\mathbb{Q}}_\ell$ and

(a)" $\mathrm{End}_{\overline{\mathbb{Q}}_\ell, G_\Gamma} V_\sigma = \overline{\mathbb{Q}}_\ell$ and V_σ is a simple $\overline{\mathbb{Q}}_\ell[G]$-module.

For any L/K finite, any place w of L at which X L has good reduction, let $a_w = \mathrm{tr}(\rho_\lambda(F(w))$ is defined (independent of λ). So we can define the Frobenius field F_L attached to X and L: $F_L = \mathbb{Q}(a_w$: these w). $F \subset E$ because $a_w \in E$ for each w (E-rational). It reflects the property of ρ_λ as can be seen from the Cebotarev theorem and representation theory. In fact:

(b) For $\sigma, \tau \in \overline{\Gamma}$, $V_\sigma \approx V_\tau$ as $\overline{\mathbb{Q}}_\ell[G]$-modules iff $\sigma|_{\overline{F}_L} = \tau|_{\overline{F}_L}$.

Combine these facts together, we have:

(c) $\mathrm{End}_{\overline{\mathbb{Q}}_\ell, G_\Gamma} \overline{V}_\ell$ is a semi-simple $\overline{\mathbb{Q}}_\ell$-algebra with center $F \otimes \overline{\mathbb{Q}}_\ell$; it is also a free $\overline{E}_\ell$-module of rank $[E:F_L]$.

Using a rationality argument (Galois theory) we also have

(c)' $\mathrm{End}_{G_\Gamma} V_\ell = \mathrm{End}_{\mathbb{Q}_\ell, G_\Gamma} V_\ell$ is a semi-simple $\mathbb{Q}_\ell$-algebra with center $F \otimes \mathbb{Q}_\ell$; it is also a free E_ℓ-module of rank

$[E:F_L]$.

If we let $F = \cap F_L$, then we can see

(d) $\mathrm{End}_{\mathcal{G}} V_\ell = E_\ell$ iff $F = E$ iff $F_L = E$ for any L.

We can now state our aim

Theorem $\mathrm{End}_{\mathcal{G}_\ell} V_\ell = E_\ell$ iff $\mathcal{G}_\ell = \mathfrak{h}_\ell$.

Remark The statement is reasonable. $\mathrm{End}_{\mathcal{G}} V_\ell \supseteq E_\ell$ as is certainly that $\mathcal{G}_\ell$ acts E-linarly. The equality means $\mathcal{G}_\ell$ has enough operators. On the other hand $\mathfrak{h}_\ell$ is the largest Lie algebra with this property.

Proof. Assume $\mathrm{End}_{\mathcal{G}_\ell} V_\ell = E_\ell$. Hence $\mathrm{End}_{\overline{\mathcal{G}}_\ell} \overline{V}_\ell = \overline{E}_\ell$. Let's show $\overline{\mathcal{G}}_\ell = \overline{\mathfrak{h}}_\ell$ instead. Recall the decomposition

$$\overline{\mathcal{G}}_\ell = \prod_{\overline{\tau}} \mathcal{G}_\sigma$$

similar to that after (a)'. Then we have first $\mathrm{Eng}_{\mathcal{G}_\sigma}(V_\sigma) = \overline{\mathbb{Q}}_\ell$ according to the decomposition of $\mathrm{End}_{\mathcal{G}} \overline{V}_\ell = \overline{E}_\ell$. By the semi-simplicity of the action of G we have

$$\mathcal{G}_\sigma = \mathrm{gl}(V_\sigma) \quad \text{or} \quad \mathrm{sl}(V_\sigma).$$

It must be that $\mathcal{G}_\ell = \mathrm{gl}(V_\sigma)$. Now we use the "two principal". For $\sigma \neq \tau$, to show the projection of $\mathcal{G}_\ell$ to $\mathrm{gl}(V_\sigma) \times \mathrm{gl}(V_\tau)$ is the as that of $\mathfrak{h}_\ell$. The reason is, if not, the Coursat

lemma will show that V_σ and V_τ will become isomorphic as $\mathcal{J}_\ell$-modules. That will imply $\mathrm{Eng}_{\mathcal{J}} V_\ell$ not commutative (in view of the above decomposition, contradictary to the disscusion in §11.1). Then we apply thm.25A.

11.2. Equality between the Lie algebras.

Under the same assumption (2) and (3) of (RM) in §11.0 we can prove that X is in fact a parametrized Abelian variety (Ribet [2] prop. §3.6.1) and (ii) of §11.1 holds (Lemma 4.5.1, loc. cit.). So does (i) of §11.1 (thm 4.2.1 & 4.3.1, loc. cit.). These ((i) and (ii)) are fundamental. Assume moreover (1) of (RM) of §11.0 holds. In this case

Theorem 30. (thm 4.5.4, loc. cit.) $\mathcal{J}_\ell = \mathfrak{h}_\ell$.

In fact, a priori according to the analysis in §11.1, with the same notation there, if the consideration (i) and (ii) there are satisfied (this is so particularly when X is described as in the beginning of this section), we have

Proposition 31. (Ribet [2] thm.4.5.3) The following conditions are equivalent (with the same notations as in §11.1):

(a) $\rho_\ell = \rho'_\ell$ for one ℓ;

(b) $\rho_\ell = \rho'_\ell$ for all ℓ;

(c) $E = F$;

(d) $E = F_L$ for all quadratic extensions L of K which is unramified outside the set of places where X has bad reduction;

(e) There exists a place v of K at which X has good reduction such that a_v^2 generates E over $\mathbb{Q}$ where $a_v = \mathrm{tr}(\rho_\ell(F(v)))$.

Very roughly (or superficially), the proof of thm.30 is to find a place v at which X can be viewed as a parametrized Abelian variety. Then one applies the knowledge of the these varieties (cf. Ribet [2] III) to obtain the result ((c) of prop.31, (c)' of §11.1: to show $[E:F] = 1$).

11.3. The Lie group.

We have finally (the reduction version)

Theorem 32. (Ribet [2] thm.5.5.2) Under the condition (RM) in the beginning of this section (from which (i) and (ii) of §11.1 can be derived), the map $\rho_\lambda^{\sim}: G \longrightarrow \mathrm{Aut}(X_\lambda)$ is surjective for almost all λ. Hence by Coursat's Lemma (or "2-principal") the map $\rho_\ell^{\sim}: G \longrightarrow \mathrm{Aut}(X_\ell)$ is also surjective for almost all ℓ.

12. A related result of Ohta.

As we have mentioned in the introduction, the results seem quite far from complete. We state another case here.

First are some notations. Let B be an indefinite quaternion algebra over $\mathbb{Q}$, D a maximal order of B. Assume that A is a 2-dimensional Abelian variety defined over a number field K such that $\mathrm{End}_K(A) \approx D$. Then similar to the discussion for CM in §1.7, we have

$$\rho_\ell : G \longrightarrow \mathrm{Aut}_D(T_\ell(A)) \approx D_\ell^\times$$

where as usual $D_\ell = D \otimes \mathbb{Z}_\ell$.

In Ohta [1], he proves the following result:

Theorem 33. (a) $\rho_\ell(G) = G_\ell$ is an open subgroup of $D_\ell^\times$ for all ℓ; (b) $G_\ell = D_\ell^\times$ for almost all ℓ.

Such an A everywhere has potential good reduction. The results for A relating to its reduction at each prime similar to those of elliptic curves still hold. We do not reproduce it here as "The proof proceeds almost in the same way as Serre's papers [2], [6] and [8]" (p.299, Ohta [1]).

13. Abelian varieties with CM.

Assume X is an Abelian variety defined over a field K with CM by a field F of degree $2\dim X$ over $\mathbb{Q}$ and that all endomorphisms of X are defined over K. Such an X everywhere has potential good reduction. Let $R = F \cap \mathrm{End}(X)$, which is an order in F. Then as in §1.3 and §1.7, the $\mathfrak{l}$-adic representation induces:

$$\rho_{\mathfrak{l}} : G \longrightarrow R_{\mathfrak{l}}^{\times}.$$

In particular, $G_{\mathfrak{l}}$ is Abelian. For Tate's module we have

Proposition 34. (Serre & Tate [1] thm.5) $V_{\mathfrak{l}}$ is a free $F_{\mathfrak{l}}$-module of rank 1.

This implies particularly that the commutant of R in $\mathrm{End}(V_{\mathfrak{l}})$ is $F_{\mathfrak{l}}$. And $C_{\mathfrak{l}} \subseteq F_{\mathfrak{l}} = F \otimes \mathbb{Q}_{\mathfrak{l}}$.

Since all endomorphisms of X are defined over K, related to its Lie algebra of the Abelian variety, there is an algebraic group morphism (K is a number field now)

$$\Phi : T_{K/\mathbb{Q}} \longrightarrow T_{F/\mathbb{Q}}$$

(see §7, Serre & Tate [1] as well §5 of chapter I) One has by taking $\mathbb{Q}$, $\mathbb{Q}_\ell$ and $\mathbb{R}$ points respectively the maps:

$$\Phi : K^\times \longrightarrow F^\times$$
$$\Phi_\ell : K_\ell^\times \longrightarrow F_\ell^\times$$
$$\Phi_\infty : K_\infty^\times \longrightarrow F_\infty^\times$$

Then the general version of Lemma 7 can be stated as

Lemma 7' (Serre & Tate [1] thm.11) There exists a unique homomorphism

$$\xi : I \longrightarrow F^\times$$

such that for any ℓ $\varphi_\ell(a) = \xi(a)\,\Phi(a_\ell^{-1})$.

Therefore our knowledge about the image G_ℓ is just that of ξ and Φ.

There is an interpretation of the ℓ-adic representation by the algebraic representation of some Serre's group S_m defined in Chapter I. In fact, if T is the torus attached to F, we see (cf. chap. I) the ℓ-adic representation are realized by

$$\rho_\ell : G \longrightarrow T(\mathbb{Q}_\ell) = F_\ell^\times$$

It is clear (in fact difficult)

Theorem 35. (Serre [6] II §2.8 thm.1) The system (ρ_ℓ) of ℓ-adic representations of K is strictly compatible with values in T and is induced by an algebraic morphism of a Serre's group

$$S_m \longrightarrow T$$

(with some module m) in the sense of §5, chapter I.

Remark For the ℓ-adic representation theoretic properties of (ρ_ℓ), cf. theorem of §1.3.1.

Part III ℓ-adic representations attached to Modular Forms

1. Modular Forms.

1.1. Congruence subgroups.

We will use σ universally in §1 to denote a 2x2 matrix:

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Recall the usual notations:

$$GL(2,\mathbb{R})^+ = \{ \sigma \in GL(2,\mathbb{R}) : \det(\sigma) > 0 \}$$
$$\Gamma(N) = \{ \sigma \in SL(2,\mathbb{Z}) : a \equiv d \equiv 1,\ b \equiv c \equiv 0 \pmod{N} \}$$
$$\Gamma_0(N) = \{ \sigma \in SL(2,\mathbb{Z}) : c \equiv 0 \pmod{N} \}$$
$$\Gamma_1(N) = \{ \sigma \in \Gamma_0(N) : a \equiv d \equiv 1 \pmod{N} \}$$

$\Gamma(N)$ is called the principal congruence subgroup of level N. A congruence subgroup of level N is a subgroup of $SL(2,\mathbb{Z})$ which contains $\Gamma(N)$.

Let H be the upper half plane $\{ z \in \mathbb{C} : Im(z) > 0 \}$. Then $GL(2,\mathbb{R})^+$ acts on H by

(1) $\quad z \longmapsto (az+b)/(cz+d) = \sigma(z)$

So do the Γ's. Hence these groups act on the space of meromorphic functions on H, as follows. For a meromorphic function f, $\sigma \in GL(2,\mathbb{R})^+$ and k an integer we write

(2) $\quad f|[\sigma]_k = \det(\sigma)^{k/2} f(\sigma(z))(cz+d)^{-k}$.

1.2. Forms with nebentypus.

A modular function for a congruence subgroup Γ of level N of weight k is a meromorphic function f on H such that

(a) f is invariant under Γ, i.e., $f|[\sigma]_k = f$ for any $\sigma \in \Gamma$;

(b) f is meromorphic "at infinity", which is explained as follows. Since Γ contains $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ by (a) $f(z+N) = f(z)$. Therefore f admits a Fourier expansion:

$$f(z) = \sum a_n q^n \quad \text{where } q = \exp(2\pi iz/N) \quad (\text{Jacobi } q).$$

Then "meromorphic at ∞" means that this expansion has only finitely many non-zero terms with negative index.

A modular form is a modular function holomorphic on

H and "at ∞". A cusp form is a modular form which "vanishes at ∞".

Let $M(\Gamma,k)$ denote the linear space of modular forms of weight k for Γ; $S(\Gamma,k)$ the subspace of cusp forms. They have finite dimension over $\mathbb{C}$. (cf. Shimura [1] or Harvey [1])

Example Let L be a lattice in $\mathbb{C}$ and

$$\wp(z) = z^{-2} + \sum_{L\setminus\{0\}}{}'((z-w)^{-2} - w^{-2})$$

$\wp(z)$ is an (elliptic) function on the elliptic curve $\mathbb{C}/L$, and is called the Weierstrass' $\wp$-function. Together with

$$\wp'(z) = -2\sum_{L}(z-w)^{-3}$$

the pair $\wp$ and $\wp'$ gives a parametrization of $\mathbb{C}/L$:

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

for some g_2 and g_3. Expand $\wp$ into power series

$$\wp(z) = z^{-2} + \sum_{k=0}^{\infty}(2k+1)G_{2k+2}z^{2k}$$

where $G_k = \sum' w^{-k}$; they are called Eisenstein series'. The Eisenstein series G_k is a modular form for $SL(2,\mathbb{Z})$ of weight k if $k \geq 2$. We have

$$g_2 = 60G_4, \quad g_3 = 140G_6.$$

Then

Theorem The graded algebra $\bigoplus_k M(SL(2,\mathbb{Z}),k)$ (naturally) is just $\mathbb{C}[g_2,g_3]$ as a polynomial ring.

Let

$$\Delta = g_2^3 - 27g_3^2 \quad \text{and} \quad j = (12g_2^3) / \Delta.$$

j is of weight 0. In fact $\mathbb{C}(j)$ is the function field of the Riemann sphere S^2 and also is the field of all modular functions of weight 0 (for $SL(2,\mathbb{Z})$).

The Fourier expansion of G_k is

$$G_k = -B_k/k! + 2/(k-1)! \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n$$

where σ_{k-1} is the divisor function and the normalized Eisenstein series is

$$E_k = -k!/B_k\, G_k.$$

E_k has integral coefficients (von Staudt-Kummer).

$$\Delta(z) = e^{2\pi iz} \prod_m (1 - e^{2m\pi iz})^{24}$$

is a cusp form of weight 12 for $SL(2,\mathbb{Z})$. Its Fourier expansion is

$$\Delta(z) = \sum \tau(n)\, q^n$$

where $\tau(n)$ is known as Ramanujan's function.

1.2.1 We consider forms in $M(\Gamma_1(N),k)$. They may not be invariant under the action of $\Gamma_0(N)$. However if $\sigma \in \Gamma_0(N)$ σ acts on $M(\Gamma_1(N),k)$ depending only on d. Because of this reason we write the operator R_d for the action: $f|[\sigma]_k = f|R_d$. In fact

$$f|R_d = \xi(d)\, f$$

where ξ is a mod N Dirichlet character and

$$M(\Gamma_1(N),k) = \bigoplus_{\xi} M(\Gamma_0(N),k,\xi).$$

Here we have used the notation $M(\Gamma,k,\xi)$ for a character ξ of Γ to denote the space of forms f such that $f|[\sigma]_k = \xi(\sigma)f$. Because of this reason we will study forms in $M(\Gamma_0(N),k,\xi)$ instead. We asy f is of type (k,ξ). ξ is also called a nebentypus. Note $\xi(-1) = (-1)^k$ otherwise $M(\Gamma_0(N),k,\xi) = 0$.

1.3. Hecke Operators, Eigenforms and Euler product.

1.3.1 $S(\Gamma,k)$ becomes a finite dimensional Hilbert space

under the Petersson inner product

$$(f, g) = \frac{1}{h} \iint_D f(z)\overline{g(z)}y^{k-2}\,dxdy$$

where $h = [SL(2,\mathbb{Z}):\Gamma]$, $z=x+iy$ and the integration is taken over a fundamental region D of Γ.

1.3.2 Assume $f = \sum a_n q^n$ is a modular form for $\Gamma_1(N)$ of type (k,ξ). The Hecke operators T_p are defined by

$$f|T_p = \sum a_{np}q^n + \xi(p)p^{k-1}\sum a_n q^n \qquad \text{if } p \nmid N;$$
$$f|T_p = \sum a_{np}q^n \qquad \text{if } p \mid N.$$

The T_p act on $M(\Gamma_0(N),k,\xi)$ and on $S(\Gamma_0(N),k,\xi)$ which are also unitary operators on the latter space with respect to the Petersson inner product.

The Hecke operators form a commutative ring and commute with R_d. In particular $S(\Gamma_0(N),k,\xi)$ has a basis consisting of eigenforms for the Hecke operators simultaneously. For such a form f, we have

$$f|T_p = c_p f \qquad \text{for } c_p \in \mathbb{C} \text{ and } p \nmid N.$$

If a cusp form f has a normalized Fourier expansion (i.e. $a_1 = 1$) then $a_p = c_p$. All a_p are algebraic integers. They generate a finite extension over $\mathbb{Q}$. We have also

(3) $$a_p = \overline{a_p}\,\xi(p)$$

from the action of R_d.

1.3.3. Newforms.

$M(\Gamma_1(M),k) \subsetneq M(\Gamma_1(N),k)$ if $M|N$. If a form f in $M(\Gamma_1(N),k)$ "is not" a form of lower level we say it is a new form. This identification is compatible with T_p and R_d. The fact is, $M(\Gamma_1(N),k)$ is decomposed into the direct sum of the subspaces of newforms of all lower levels dividing N.

1.3.4 The Hecke operators formally satisfy an Euler product relation (for the definition of general T_n see Shimura [2] or Harvey [1]):

$$\sum_{n=0}^{\infty} T_n n^{-s} = \prod_{p\nmid N} \left(1-a_p p^{-s} + \xi(p)p^{k-1-2s} \right)^{-1} \prod_{p|N} \left(1-a_p p^{-s} \right)^{-1}.$$

Hence for an eigenform $f = \sum a_n q^n$ which is also a new form its Mellin transform (i.e. the associated Dirichlet series) also has an Euler product:

$$L_f(s) = \sum a_n n^{-s} = \prod_{p\nmid N} (1-a_p p^{-s}+\xi(p)p^{k-1-2s})^{-1} \prod_{p|N} (1-a_p p^{-s})^{-1}.$$

This amounts to the same as a recurrence relation:

$$a_n \cdot a_m = a_{nm} \qquad \text{if } (m, n) = 1;$$
$$a_{p^{r+1}} = a_p a_{p^r} - \xi(p)p^{k-1} \cdot a_{p^{r-1}} \qquad \text{if } p \nmid N$$

1.4. Functional Equation and Petersson Conjecture.

1.4.1 Note first for an automorphism $\phi \in \mathrm{Aut}(\mathbb{C})$ we have that

$$f^{\phi} = \sum a_n^{\phi} q^n$$

is also a form in $M(\Gamma_1(N),k)$ if f is. Put

$$\Lambda_f(s) = N^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L_f(s)$$

we have the functional equation:

$$\Lambda_f(s) = A \cdot \Lambda_{\bar{f}}(k-s)$$

for some $A \in \mathbb{C}$.

1.4.2 Assume again $f = \sum a_n q^n$ is a newform of $M(\Gamma_1(N),k)$ which is also an eigen cusp form with eigenvalues a_p. Then the Petersson's conjecture claims:

$$| a_p | < 2p^{\frac{1}{2}(k-1)}.$$

2. The mod ℓ theory.

Most of the results here are about the forms for $SL(2,\mathbb{Z})$ (Reference: Swinnerton-Dyer [1], Serre [7], Ribet [1] and Katz [1] & [2])

2.1. Forms and Fourier expansion.

Assume $M(R,k)$ is the linear space of modular forms of weight k with coefficients in a ring R (cf. Katz).

For each $f \in M(R,k)$, f has the q (or Fourier)-expansion:

$$f = \sum a_n q^n \in R[[q]].$$

2.2. Scalar extension and reduction.

For a ring homomorphism $h: R \longrightarrow R'$, we have

$$M(R,k) \otimes R' \longrightarrow M(R',k)$$

via $(\sum a_n q^n) \otimes b \longmapsto \sum h(a_n) b q^n$.

2.2.1 Katz: If $R = \mathbb{Z}$, $1/6 \in R'$, then the above map is an isomorphism.

Example For a prime $\ell \geq 5$, we have

$$\begin{array}{ccc} M(\mathbb{Z},k) & \longrightarrow & M(\mathbb{F}_\ell,k) \\ \downarrow & \nearrow & \\ M(\mathbb{Z},k) \otimes \mathbb{F}_\ell & & \end{array}$$

is the "mod ℓ" reduction. Serre and Swinnerton-Dyer have adopted this as the definition of the mod ℓ forms.

2.3. The q-expansion principle of Katz.

If $R \subseteq R'$, $f \in M(R',k)$ has q-expansion with coefficients in R, then $f \in M(R,k)$.

2.4. The structure theorem of Swinnerton-Dyer.

$\mathbb{F}_\ell$ denotes the field of ℓ elements and $\overline{\mathbb{F}}_\ell$ its algebraic closure. We will from now on let $\overline{M}(k) = M(\overline{\mathbb{F}}_\ell,k) = M(\mathbb{F}_\ell,k)\otimes\overline{\mathbb{F}}_\ell$ if $\ell \geq 5$.

Let $A \in M(\ell-1)$ be the image of $E_{\ell-1}$, the normalized Eisenstein series. Then $A = 1$. But multiplication by A gives

$$M(k) \longrightarrow M(k+\ell-1).$$

2.4.1 Let $f \in \overline{M}(k)$, $f' \in \overline{M}(k')$, having the same q-expansion, then $k \equiv k' \pmod{\ell-1}$ and $f = A^n f'$ with $n = (k-k')/(\ell-1)$. This is the structure theorem of Swinnerton-Dyer.

2.4.2 Remark In Swinnerton-Dyer [1] and Serre [7], theorem (2.4.1) appears in the following form:

$M = \sum M(k) = \mathbb{F}_\ell[Q,R]/(A-1)$ where $Q = A_4$, $R = A_6$, and $A = A(Q,R)$, and $\mathbb{F}[Q,R]$ has been viewed as a polyno-

mial ring (see theorem of §1.2). M has a natural grading $\mathbb{Z}/((\ell-1))$.

2.5. Filtration.

This will be the main tool. For $f \in \overline{M}(k)$, let

$$w(f) = \inf \{ k' : g \in \overline{M}(k') \text{ such that } g \text{ \& } f \text{ have the same q-expansion} \}.$$

The basic properties, which follow easily, are:

(i) $w(0) = \infty$;

(ii) w depends only on the q-expansion;

(iii) if $f \neq 0$, $f \in M(k)$ then $w(f) \equiv k \pmod{\ell-1}$.

Theorem 1. There is a unique map

$$\Theta : M(k) \longrightarrow M(k+\ell+1) \quad ,$$

which induces the action on the q-expansions by $q(d/dq): \sum a_n q^n \mapsto \sum n a_n q^n$. If $w(f) = k$ and $\ell \nmid k$, then $w(\Theta(f)) = k+\ell+1$.

One sees in particular if $\ell > k$ then Θ is one-one.

The following results are used in applying the theory to obtain boundedness (for the exceptional primes, cf. §4.3 below) of ℓ under certain conditions.

(1) Let $f \in M(k)$, $g \in M(k')$, both non-zero, $k \geq k'$. If $t > 0$ is an integer such that $a_n(f) = n^t a_n(g)$, for all n prime to N then $t \equiv \frac{1}{2}(k-k') \pmod{\ell-1}$ or $t \equiv \frac{1}{2}(k-k'+\ell-1) \pmod{\ell-1}$. Moreover if $\ell \geq k+k'$, then $k = k'$, $f = g$ and $(\ell-1) \mid t$.

(2) $f \in M(k)$ non-zero, $a_n(f) = 0$ for $(\frac{n}{\ell}) = -1$. Then $2k > \ell$.

(3) If $f \in M(k)$ is a "cusp" form, i.e. $a_0 = 0$, and there are $\bmod(\ell-1)$ integers m and m' such that $m+m' \equiv k-1 \pmod{\ell-1}$ and $a_n \equiv n^m \sigma_{m'-m}(n) \pmod{\ell}$ when $(n,\ell)=1$, then $\ell \leq k+1$ or, ℓ divides the numerator of B/k, where B is the Bernoulli number (appearing in G_k).

2.6. Remark.

Katz has generalized the theory to arbitrary coefficient ring and arbitrary level, where the normalized Eisenstein series is replaced by the Hasse invariant. This will be used in the determination of the image in the group level, in §11.

3. Data: the ℓ-adic representation attached to a cusp form.

3.1. The representation.

For $f = \sum a_n q^n \in S(\Gamma_1(N),k)$, let $K = \mathbf{Q}(a_n)$. K is a finite extension of $\mathbf{Q}$. Put $\Gamma = \{\sigma : K \longrightarrow \mathbb{C}\}$. Assume f is an eigen newform of type (k,ξ).

Starting from such an f we have then a continuous representation, due to Deligne-Serre:

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}(2, K\otimes\mathbf{Q}_\ell).$$

This ℓ-adic representation ρ_ℓ is

(i) unramified outside ℓN;

(ii) $\mathrm{tr}(\rho_\ell(F(p))) = a_p$, $\det(\rho_\ell(F(p))) = \xi(p)p^{k-1}$ for $p \nmid \ell N$.

One sees easily that the system is rational strictly compatible with exceptional set $\subseteq N$.

3.2. A decomposition.

As shown in §10.1 of chapter I for $K\otimes\mathbf{Q}_\ell = \prod_{\lambda|\ell} K_\lambda$, we have the λ-adic representations:

$$\rho_\lambda : G \longrightarrow \mathrm{GL}(2,K_\ell) \longrightarrow \mathrm{GL}(2,K_\lambda)$$

then $\rho_\ell = \prod \rho_\lambda$, cf. Ribet [3]. Therefore we can consider λ-adic representations as well as ℓ-adic ones.

3.3. Remark.

In [2] Ohta has constructed ℓ-adic representations for F attached to an algebraic representation

$$\rho : B \longrightarrow GL(m, \mathbb{Q})$$

where B is a quaternion algebra over a totally real number field F of degree g under some conditions (loc.cit. p.2). Starting from such a ρ, he constructs a space of automorphic forms and the Hecke operators on this space. The representation $\Phi_\ell : Gal(\overline{F}/F) \longrightarrow GL(n, \mathbb{Q}_\ell)$ constructed there for every ℓ are unramified for almost all primes and satisfy a congruence relation for the arithmetic Frobenii.

3.4. Frobenius at infinity.

A remarkable simple fact is that, if c is the complex conjugate ("Frobenius at ∞") in G, $\rho_\ell(c)$ will be of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

for some basis since its determinant is $\chi_\ell(-1)^{k-1} \varepsilon(-1) = -1$ (by considering its action).

3.5. An illustration of the content.

In what follows, after a quick review of the case of the forms for $SL(2,\mathbb{Z})$ in §4, in §5-6 we follow Ribet [3] to treat some general properties of the representations attached to modular forms obtained above by Deligne-Serre. The mod ℓ theory plays an important role in the consideration in §4. But it does not concern with the content of §5-10. Theorem 7 leads to 2 situations which we have to consider separately, namely forms do or do not have complex multiplication (definition §6.1). The former case is discussed in §7 and §9. In §8 we will take a glance at the case $k = 1$. In §10 we consider the Lie algebra of the representation according to Ribet and Momose. In §11 we return to the group level after Ribet. This is the occasion we encounter again the mod ℓ theory.

4. A review of the simplest case: eigenforms for $SL(2,\mathbb{Z})$ (Serre, Swinnerton-Dyer, Ribet).

For the basic properties, cf. §5 below.

4.1. The represetation and the problems.

As $\det \rho_\ell = \chi_\ell^{k-1}$ where χ_ℓ is the cyclotomic

character (see Part I §3 (a)) which maps G onto $\mathbb{Z}_\ell^\times$, we have

$$G_\ell \overset{\Delta}{=} \text{image of } \rho_\ell \subseteq \{u \in GL(2,\mathbb{Z}_\ell) : \det(u) \in \mathbb{Z}_\ell^{\times k-1}\} \overset{\Delta}{=} A_\ell .$$

The basic facts (or problems) are:

(1) G_ℓ is open in A_ℓ for all ℓ; (note A_ℓ is open in $GL(2,\mathbb{Z}_\ell)$

(2) $G_\ell = A_\ell$ for almost all ℓ.

4.2. Openness problem (1).

In Serre [4], he has considered the representation attached to Δ (see §1.2), the only cusp form of weight 12. He proves (1) in this case, using the theory of Abelian ℓ-adic representations, and claims his result holds for other cusp forms (§5.1 & §5.3). This is a fact.

Let's consider (1). Following is the proof. First by semi-simplification we assume ρ_ℓ is semi-simple. Then the Lie algebra $\mathcal{G}_\ell = \mathcal{S} \times \mathcal{C}$ with $\mathcal{C}$ Abelian and $\mathcal{S}$ semi-simple. If $\mathcal{S} \neq 0$ then $\mathcal{S} = sl(2,\mathbb{Q}_\ell)$. But $\mathcal{G}_\ell \subsetneq sl(2,\mathbb{Q}_\ell)$ so $\mathcal{G}_\ell = gl(2,\mathbb{Q}_\ell)$. It suffices to exclude $\mathcal{S} = 0$. If so and $\mathcal{C} = \mathbb{Q}_\ell$ = center of $gl(2,\mathbb{Q}_\ell)$, the data will give, $4p^{11} = \tau(p)^2$ for infinitely many p. This is impossible. Therefore $\mathcal{S} = 0$ and $\mathcal{C} \neq \mathbb{Q}_\ell$. The commutant of $\mathcal{G}_\ell$ is a non-split Cartan algebra. Then ρ_ℓ restricted on the open subgroup of index ≤ 2 is Abelian. The whole system (ρ_ℓ)

when restricted on this open subgroup is locally algebraic by the theorem of Serre and Lang and the semi-simplicity as it is rational and is strictly compatible. Hence they come from a Serre's torus. (cf. also thm.17, Part I) In particular the G_ℓ's contain an open Abelian subgroup of index ≤ 2. If (1) fails for an ℓ because of the above mentioned reason, all will have this property.

Now shown by Shimura [2], the reduction mod 11 of ρ_{11} is isomorphic to the one of an elliptic curve with image the whole $GL(2,\mathbb{F}_{11})$, which leads to a contradiction.

4.3. Exceptional primes.

In Serre [7] and Swinnerton-Dyer [1], they turn to consider the "exceptional primes", still they assume $a_n \in \mathbb{Z}$.

An exceptional prime is a prime number ℓ at which $G_\ell \not\supseteq SL(2,\mathbb{Z}_\ell)$. (See the 2nd paragraph of §4.2) In particular $G_\ell = A_\ell$ if ℓ is not exceptional. Group theory then shows, by explicitly considering the image, this is just some congruence relations among the a_n's. This fact can be expressed by equalities of mod ℓ forms. So the mod ℓ thoery gives bounds on ℓ, i.e., (2) of §4.1 holds.

Let's look into more detail. Consider the reduction (which means the same). For $G_\ell^{\sim} = \operatorname{im} \rho_\ell^{\sim} \not\supseteq SL(2,\mathbb{F})$, by thm.10A & 11A we have the following possibilities:

(a) $G_\ell^{\sim} \subseteq$ some Borel subgroup;

(b) There is a Cartan subgroup C with normalizer N such that $G_\ell^{\sim} \subseteq N$ but $G_\ell^{\sim} \not\subseteq C$;

(c) $H_\ell = \mathrm{im}(G_\ell^{\sim} \longrightarrow \mathrm{PGL}(2)) \simeq A_4$, S_4 or A_5.

which will imply respectively the following congruence relations:

(a)' $\exists$ m such that $a_n \equiv n^m \sigma_{k-1-2m}(n) \pmod{\ell}$ if $(n,\ell) = 1$;

(b)' $a_n \equiv 0 \pmod{\ell}$ if $\left(\frac{n}{\ell}\right) = -1$;

(c)' $p^{1-k} a_p^2 \equiv 0, 1, 2$ or $4 \pmod{\ell}$ if $p \neq \ell$.

Now (a)' and (b)' are easily referred to §2.5. (c)' is direct to give a bound of the ℓ's.

This is indeed an interesting thing when Ramanujan's congruence relations for his $\tau(n)$ are related to the representations, e.g.

$$\tau(p) \equiv p + p^4 \pmod{7}.$$

4.4. Forms with arbitrary coefficients.

In [1], Ribet gives the complete description for the forms of $\mathrm{SL}(2,\mathbb{Z})$ with arbitrary coefficients. Note in this case A_ℓ is in fact

$$A_\ell = \left\{ u \in \mathrm{GL}(2, \mathcal{O} \otimes \mathbb{Z}_\ell) : \det(u) \in \mathbb{Z}_\ell^{\times k-1} \right\}$$

where O (it also appears as the ring of Hecke operators) is the ring of integers of K (see §3.2).

To see this, again reduce to considering the semi-simplification of the mod ℓ reduction of the representation. Writing

$$G_\ell^{\sim} = \prod G_\lambda^{\sim} \subseteq \prod GL(2,O/\lambda) = GL(2,O/\ell O)$$

one can concentrate on a single prime ideal λ at first. Ribet hence reduces the problem (2) to proving the following two conditions according to thm.18A:

(i) The group $G_\lambda^{\sim}$ has order divisible by ℓ and acts irreducibly on $(O/\lambda)^2$.

(ii) There is a $u \in G_\ell^{\sim}$ such that $(tr(u))^2$ generates the $\mathbb{F}_\ell$-algebra $O/\ell O$.

For (i), the irreducibility is obtained exactly as that in §4.3 (a) (see also §4.2.3, Part II). About the order, if upon the contrary, we have by thm.10A three possibilities listed there. (1) occurs only finitely many times because thm.4 and the first part of (i). (2) and (3) are exactly like (b) and (c) of §4.3.

Granting (i), (ii) holds at first for those primes of degree 1. In fact from thm.6A we have $G_\ell^{\sim} \supseteq SL(2,O/\lambda) \approx SL(2,\mathbb{F}_\ell)$. Then we use again "two principle". Fix any $\lambda \neq \lambda'$ over ℓ and let (temporarily) A' and G' be the

projections of A and G to

$$GL(2,O/\lambda \times O/\lambda').$$

It suffices to show $G' \supseteq SL(2,O/\lambda \times O/\lambda')$. Assume the contrary, by thm.22A, we have an

$$\varepsilon : G' \longrightarrow \{\pm 1\}$$

such that $tr(u) = \varepsilon(u,u')tr(u')$ for $(u,u') \in G'$. Let

$$\phi : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL(2,O/\lambda) \times GL(2,O/\lambda') \longrightarrow \{\pm 1\}.$$

Then unramifiedness shows either $\phi = 1$ or $\phi =$ Legendre symbol $(\frac{\cdot}{\ell})$.

In the former case the mod λ and the mod λ' forms f_λ and $f_{\lambda'}$ of f are identical. This is impossible because

$$O/\ell O \approx \prod O/\lambda$$

but the a_n's generate O. In the latter case we deduce again from mod ℓ theory that $a_n(f_\lambda) = n^{\frac{k-1}{2}} a_n(f_{\lambda'})$. Then we refer to (1) of § 2.5. We have hereby finished the consideration of the case of the prime numbers which split completely.

Consequently (from Cebotarev's Density Theorem) there are infinitely many prime p such that a_p^2 generates the field E. This follows from the fact that A itself has

such an element whose square generateing E. Now we finish the proof of (ii), as any such an a_p^2 will generate O as a ring "for almost all prime ℓ".

For (1), Ribet uses also, as Serre, the theory of Abelian ℓ-adic representation, since we already have (2), instead of $\ell = 11$ used there. cf. thm.18 of Part I.

4.5. Remark: the case of finite product.

Similar to the case of elliptic curves as Serre did, Ribet proves by the way the case for the representation which is the product of finitely many these representations, cf. also Part II, §12.3.

5. Basic Properties of the representations.

Theorem 2. $\det \rho_\ell = \varepsilon \chi_\ell^{k-1}$

Proof. This is a consequence of the Cebotarev Density Theorem, as the formula holds for the Frobenii.

Theorem 3. (Ribet [3] thm.2.3) The ρ_λ is a simple K_λ-representation.

Proof. For otherwise the semi-simplification r of will be given by two characters:

$$r = \phi_1 \oplus \phi_2 .$$

r is now a semi-simple K-rational Abelian λ-adic representation of G, hence locally algebraic by the theorem of Serre and Lang. According to Part I §8.3, these ϕ_i differ from some powers of the cyclotomic character $\chi_i^{n_i}$ by characters ξ_i of finite order unramified outside N. Write

$$\phi_i = \xi_i \phi_i .$$

Now we have

$$a_p = \mathrm{tr}(r(F(p))) = \xi_1(p)p^{n_1} + \xi_2(p)p^{n_2}$$
$$\phi_1 \phi_2 = \xi \chi_\ell^{k-1}$$

We have $\xi_1 \xi_2 = \xi$, and $n_1 + n_2 = k-1$, since χ_ℓ is of infinite order. We want hereupon to deduce something about the grouth of the a_p's.

The Petersson conjecture $|a_p| < 2p^{\frac{1}{2}(k-1)}$ shows $n_1, n_2 \leq k/2$, hence $n_1 = n_2 = (k-1)/2$. In particular k is odd. $\xi_1 \neq \xi_2$ since $\xi(-1) = -1$. It is just from these data that one can estimate then

$$\sum_{p \nmid N} |a_p|^2 p^{-s} = -2\log(s-k) + O(1) \qquad \text{as} \quad s \longrightarrow k^+.$$

In fact(*), we have firstly $|a_p|^2 = |\xi_1(p)|^2 p^{k-1} + |\xi_2(p)|^2 p^{k-1} + 2\mathrm{Re}(\xi_1(p)\overline{\xi}_2(p))\, p^{k-1} = 2p^{k-1} + 2\mathrm{Re}(\xi_1(p)\overline{\xi}_2(p))\, p^{k-1}$, if $p \nmid N$. But we have known

$$\sum p^{-1-\delta} = -\log\delta + O(1) \qquad \text{as} \quad \delta \longrightarrow 0^+$$

(Hardy & Wright [1] p.352-353). $\xi' = \xi_1 \overline{\xi_2} \neq 1$. Let

$$L(z, \xi') = \prod (1 - \xi'(p)p^{-z}).$$

So

$$\begin{aligned} \log L(z,\xi') &= -\sum \log(1-\xi'(p)p^{-z}) \\ &= \sum \xi'(p)p^{-z} + \sum O(p^{-2z}) \\ &= \sum \xi'(p)p^{-z} + O(1) \qquad \text{as} \quad z \longrightarrow 1^+. \end{aligned}$$

We know $L(1, \xi') \neq 0$ (Apostol [1] p.149) since $\xi' \neq 1$. Therefore the asymptotic behaviour of the summation is

$$\begin{aligned} \sum |a_p|^2 p^{-s} &= 2\sum p^{-s+k-1} + 2\mathrm{Re}\sum \xi'(p)p^{k-1-s} + O(1) \\ &= -2\log(s-k) + O(1) \qquad \text{as} \quad s \longrightarrow k^+. \end{aligned}$$

But according to Rankin [1] the sum is

$$-\log(s-k) + O(1) \qquad \text{as} \quad s \longrightarrow k^+.$$

From this we have a contradiction. qed.

(*) I would like to thank Dr.K.M. Tsang of the University of Hong Kong who taught me this method of the estimation.

Proposition 4. (Ribet [3] thm.4.1) G_λ is not Abelian.

Proof. This is because §3.5 and the above proposition.

The standard method of average gives

Proposition 5. The restriction of ρ_λ on every open subgroup of G is semi-simple.

Proof. G is compact, cf. Part I, §8.1.

Assume $k > 1$ in the rest of this section.

Theorem 6. (Ribet [3] thm.4.3) $\overline{G}_\lambda$ = the image of G_λ in $PGL(2,K_\lambda)$ is infinite.

Proof. The method of using L-functions is due to Serre. Assume not the case. Then there are infinitely many primes p such that, $\varepsilon(p) = 1$, p splits completely in L where $Gal(L/\mathbb{Q}) = G_\lambda$, and $\rho_\lambda(F(p))$ is scalar. Then

$$a_p^2 = 4p^{k-1}\varepsilon(p) = 4p^{k-1} .$$

for these primes. If $k-1$ is odd then all these p are ramified which is impossible. So $k-1$ is even. Write $k = 2m+1$ and $\phi = \rho_\lambda \otimes \chi_\lambda^{-m}$. Two facts $\overline{\text{im}\,\phi} = \overline{G}_\lambda$ finite and $\det \phi = \varepsilon$ together show $\text{im}\,\phi$ is finite by direct computation. The rest of the proof is to compare the L-functions of ϕ and ρ_λ.

The Artin theory gives the functional equation of L_ϕ. On the other hand L_{ρ_λ} also has a functional equation for ρ_λ is a representation attached to a newform, cf. §1.4. But $\rho_\lambda = \chi_\ell^m \otimes \phi$ gives

$$L_\phi(s-m) = L_{\rho_\lambda}(s).$$

Now L_{ρ_λ} has Γ-factor

$$(2\pi)^{-s}\Gamma(s)$$

symmetric under $s \longmapsto k-s$, from the point of view of modular functions. On the other hand L_{ρ_λ} has Γ-factor from the representation theory:

$$(2\pi)^{-s}\Gamma(s-m)$$

also symmetric under $s \longmapsto k-s$ (shifted by χ_ℓ^m). Comparing the Γ-factors we have

$$\frac{\Gamma(s)\cdot\Gamma(m+1-s)}{\Gamma(s-m)\cdot\Gamma(k-s)} = c\,A^{-s}\prod\left(1-a_i p_i^{-s}\right)^{n_i}$$

where $c, A \in \mathbb{C}$, non-zero, $a_i \in \mathbb{C}$, $n_i \in \mathbb{Z}$, p_i primes. This is impossible. In fact when $s = 1, \ldots, m$, left hand side of the above eqality has a simple zero; when $s = m+1, \ldots, 2m$, the left hand side has a simple pole. There are no other zeros and poles. This forces the right hand side to be

$$c\, A^{-s} \prod_{i=1}^{m} (1-p_i^{\cdot} p_i^{-s}) \prod_{i=m+1}^{2m} (1-p_i\, p_i^{-s})^{-1}$$

But if s takes integer values and $\longrightarrow \infty$ we see a contradiction.

The following theorem leads to two different cases.

Thoerem 7. (Ribet [3] prop.4.4) Either

(1) $\rho_\lambda | H$ is irreducible for any open subgroup H of G,

or

(2) there is some open subgroup H of index 2 in G such that for any open subgroup H', $\rho_\lambda(H')$ is Abelian iff $H' \subseteq H$.

Proof. For any open subgroup H, since $\rho_\lambda | H$ is semi-simple, we see:

$$\rho_\lambda | H \text{ not irreducible} \Longrightarrow \text{diagonalized} \Longrightarrow \text{Abelian.}$$

So if (1) is not true, then there is an open subgroup on which ρ is Abelian. Then a group lemma thm.17A together with thm.8 shows the desired results.

6. Complex multiplication.

Let's consider more carefully. Suppose we have two eigenforms f and f', with weights k, k', levels N, N', eigenvalues a_p, a'_p, nebentypi ξ, ξ', representations ρ_ℓ, ρ'_ℓ, respectively.

Proposition 8. (Ribet [3] thm. §3) If $a_p = a'_p$ for a set of primes of density 1, then $k = k'$, $a_p = a'_p$ for all p prime to NN', $\xi(d) = \xi'(d)$ if $(d, NN') = 1$.

Proof. This is because Cebotarev's Density Thoerem and the fact that two representations having same trace in characteristic 0 are isomorphic (lemma 2 of §2.6, Part I).

One sees from the proof that the field $K = \mathbb{Q}(a_n)$ contains the values $\xi(d)$ for $d \nmid N$.

We proceed.

Proposition 9. (Ribet [3] prop.3.2) Let L be the largest totally real subfield of K. Then either L = K or K is an imaginary quadratic extension of L (i.e. K is a CM field).

Proof. For $\sigma \in \mathrm{Aut}(\mathbb{C})$, consider $\sigma(f)$ we have ((3) of §1.3.2)

$$\sigma(a_p) = \overline{\sigma(a_p)}\,\sigma(\xi(p))$$

But $a_p = \overline{a}_p \xi(p)$ acted by σ gives

$$\sigma(a_p) = \sigma(\overline{a}_p)\sigma(\varepsilon(p))$$

This means σ commutes with the complex conjugate on K. Then K is a CM field if $K \neq L$, cf. Shimura [1].

One sees easily (cf. (3) of §1.3.2)

Proposition 10. (Ribet [3] prop.3.3) K is a CM field unless ε is of order 2 and

(*) $\quad \varepsilon(p)a_p = a_p \quad$ for $\quad p \nmid N$

Conversly, (*) implies that K is totally real.

6.1. The definition.

Let f be as above, ϕ be a mod D Dirichlet character. Then

$$f \otimes \phi = \sum \phi(n) a_n q^n$$

is a modular form of the same weight k on $\Gamma_0(ND^2)$ of nebentypus $\varepsilon\phi^2$. Actually f is an eigenform. $\rho_{f\otimes\phi} \simeq \rho_f \otimes \phi$.

Definition. For $\phi \neq 1$, say f has complex multiplication by ϕ if,

$$\phi(p)a_p = a_p$$

for a set of primes p of density 1.

Remark. The proof of thm.10 indicates that "primes of density 1" can be replaced by "all primes outside DN". f has CM by ϕ means the same as the representations attached to $f\otimes\phi$ and f are isomorphic. One can prove in this case $\varepsilon\phi^2 = \varepsilon$. So ϕ is of order 2. If F is the quadratic field corresponding to ϕ we also say f has CM by F.

Example If $\varepsilon \neq 1$ and $K = L$ then f has CM by ε. ((3) § 1.3.2)

7. Modular forms with complex multiplication.

Theorem 11. (Ribt [3] prop.4.4) If (2) of thm.7 occurs, F is the quadratic extension for H, then F is unramified outside N, f has CM by F. Conversely, if f has CM by F then the restriction of ρ on $\mathrm{Gal}(\overline{Q}/F)$ is Abelian.

Proof. At this time, there is a Cartan subgroup C of $GL(2,K_\lambda)$ with normalizer N such that $[G : G\cap C] = 2$. Now we have

$$\phi : G \longrightarrow G/H \approx N/C = \{\pm 1\}$$

where ϕ corresponds to H or F which is obviously unramified outside ℓN (as is induced by ρ_ℓ).

But if $s \notin N \backslash C$ then $tr(s) = 0$. So if $g \in G$ such that $\phi(g) = -1$, then $tr(\rho_\ell(g)) = 0$. Hence

$$a_p = 0 \quad \text{if} \quad p \nmid N \quad \text{and} \quad \phi(p) = -1.$$

This just means f has CM by ϕ.

Conversely, let $H = \ker(\phi)$. As $\rho_\lambda \approx \rho_\lambda \otimes \phi$ there is a matrix $M \in GL(2, K_\lambda)$ such that

$$M^{-1} \rho_\lambda(g) M = \phi(g) \rho_\lambda(g).$$

That there are some $g \notin H$ implies M is not a scalar and actually semi-simple since $\phi(g) = -1$. The commutant of M in $GL(2, K_\lambda)$ is Abelian and contains $\rho_\lambda(H)$.

7.1. Concrete construction by Grossencharacters.

Let F be an imaginary quadratic field over $\mathbb{Q}$. $k > 1$. Choose an embedding $\sigma : F \longrightarrow \mathbb{C}$.

Let Φ be a Grossencharacter of F with infinite type σ^{k-1}. Let m be an integral ideal over which Φ is defined. View Φ as a homomorphism:

$$\{ \text{fractional ideal prime to } m \} \longrightarrow \mathbb{C}^\times$$

So $\tilde{\Phi}((a)) = \sigma(a)^{k-1}$ if $a \in F^{\times}$ and $a \equiv 1 \pmod{m^{\times}}$.

Let ϕ be the Dirichlet character associated to F, viewed as defined mod D, where $-D$ is the discriminant of F. Let $M = N(m)$. η is given by

$$a \longmapsto \tilde{\Phi}((a))/\sigma(a) \qquad \text{for } a \in \mathbb{Z}$$

Put $\varepsilon = \eta\phi$. Being so, let

$$g = \sum c_n q^n$$

be defined by

$$g = \sum \phi(\mathfrak{a})\, q^{N(\mathfrak{a})}$$

where the sum runs over the integral primes $\mathfrak{a}$ prime to m. Then

Thoerem 12. (Ribet [3] thm.3.4.) g is cusp form of weight k, nebentypus ε for $\Gamma_0(DM)$. It is also an eigenform with eigenvalues c_p, if $p \nmid DM$.

Remark. When g is viewed as a newform of some level dividing DM, g has CM by ϕ, for if $\phi(p) = -1$, there is no ideal $\mathfrak{a}$ such that $N(\mathfrak{a}) = p$, i.e., $c_p = 0$. (see Hecke: Lectures on the theory of algebraic numbers, thm.90)

7.2. Complete description.

Theorem 13. (Ribet [3] thm.4.5) If case (2) of thm.7 occurs, let F corresponding to H, then $\rho_\lambda|H$ is Abelian for all λ; and

(1) F is unramified outside N;

(2) F is ramified at ∞, i.e. imaginary;

(3) f is always obtained from a Grossencharacter as in §7.1.

Proof. Independent of λ comes from a theorem of the theory of ℓ-adic representations (i.e. the system comes from a Serre's torus. This can also be seen from the very definition of CM which is independent of λ .) (1) is then obvious.

$\rho_\lambda|H$ is locally algebraic because F is quadratic. So there is a representation

$$r: S_m \longrightarrow GL(2,K_\lambda),$$

giving our system of λ-adic representations (ρ_λ), where S_m is a Serre's torus associatd to F with some module m.

r is given by, over $\bar{K}$, two characters, say θ_1, θ_2. Let's write

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}/F)^{ab} & \xrightarrow{\theta_i} & \mathbb{C}^\times \\ \uparrow & \nearrow_{\Phi_i} & \\ I & & \end{array}$$

where I is the idele group of F. (Here we have chosen an embedding $K \longrightarrow \mathbb{C}$.) ϕ_i are viewed as Grossencharacters, whose conductors dividing m. ϕ_i interchange under the conjugate of $F/\mathbb{Q}$ (simply because that $\bar{\phi}$ is a character of S_m if ϕ is, and that the condition the ϕ_i satisfy. See also Weil [1]).

We have

$$(*) \qquad \phi_1 \cdot \phi_2 = \varepsilon\,(\mathrm{Norm})^{k-1}$$

(see §6.3 of Part I) where Norm is the canonical norm. For each $\mathfrak{p} \in I$, $\mathfrak{p} \nmid N(m)N$ we have

$$\mathrm{tr}(\rho_\lambda(F(\mathfrak{p}))) = \phi_1(\mathfrak{p}) + \phi_2(\mathfrak{p})$$

where $F(\mathfrak{p})$ is the Frobenius of F at $\mathfrak{p}$.

Now if F is real, then

$$\phi_i = (\mathrm{Norm})^{n_i}\,\varepsilon_i,$$

for some integers n_i and characters ε_i of finite order. Hence

$$\mathrm{tr}(\rho_\lambda(F(\mathfrak{p}))) = \varepsilon_1(\mathfrak{p})N(\mathfrak{p})^{n_1} + \varepsilon_2(\mathfrak{p})N(\mathfrak{p})^{n_2}$$

for almost all $\mathfrak{p}$. Take those p split completely in F the above equality becomes

$$a_p = \mathrm{tr}(\rho_\lambda(F(p))) = \xi_1(p)p^{n_1} + \xi_2(p)p^{n_2}.$$

Our previous proof of thm.8 shows then we must have $n_1 = n_2 = \frac{1}{2}(k-1)$. So over $\bar{K}$ the representation r can be represented as:

$$\chi_\ell^{n_1} \otimes (\xi_1 \oplus \xi_2)$$

which contradicts thm.8. Therefore F has to be imaginary, i.e. (2) holds.

Let σ and τ be the two embeddings of F in $\mathbb{C}$. If the infinite type of ϕ_1 is $\sigma^m\tau^n$, then that of ϕ_2 is $\tau^m\sigma^n$ (as seen from (*)). (*) then shows

$$m + n = k-1.$$

$m \neq n$; for otherwise, as $\theta_\lambda = (\mathrm{Norm})^m = (\sigma\tau)^m$ upto a character of finite order, our previous argument will still lead to a contradiction (to thm.8). Without loss of generalirity, assume $n > m$. Let $\phi = \phi_1(\mathrm{Norm})^{-m}$. We have

$$\prod_{\mathfrak{p}\nmid MN}(1-a_p p^{-s}+\xi(p)p^{k-1-2s})^{-1} = \prod_{\mathfrak{p}\nmid MN}(1-\phi_1(\mathfrak{p})N\mathfrak{p}^{-s})^{-1}$$
$$= \prod_{\mathfrak{p}\nmid MN}(1-\phi(\mathfrak{p})N\mathfrak{p}^{m-s})^{-1}$$

In fact for $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ over p the product

$$(1-\phi_1(\mathfrak{p})N\mathfrak{p}^{-s})\,(1-\phi_1(\bar{\mathfrak{p}})N\mathfrak{p}^{-s}) = 1-a_p p^{-s} + \xi(p)\,p^{k-1-2s}$$

as $\phi_1(\bar{\mathfrak{p}}) = \phi_2(\mathfrak{p})$. Let g be the modular form of weight n-m+1 associated to ϕ as defined in §7.1, we have

$$L_f(s) = L_g(s-m)$$

upto some Euler factors. The same contradiction as in the proof of thm.8 occurs unless $m = 0$. So f is a newform associated to $\phi = \phi_1$ in the sense of §7.1.

8. The case $k = 1$.

Before the nontrivial situation $k > 1$ we take a glance of the forms of weight 1 (Serre [9]). The obvious connection is

representation <-> Artin L-function
<-> Dirichlet series
<-> Modular form.

A special characterization in this case (i.e. $k = 1$) is that the representation has open kernel hence finite image. We view ρ_ℓ as a representation to $GL(2,\mathbb{C})$. Consider the projection of $G_\mathbb{Q}$ to $PGL(2,\mathbb{C})$, apply the results in Part IV, the image has thus three possibilities:

(a) C_n: cyclic of order n;
(b) D_n: dihedral of order $2n$, $n \geq 2$;

(c) A_4, A_5 or S_5.

In case (a) ρ_ℓ is Abelian hence reducible (over $\mathbb{C}$), other cases are not (§3 loc. cit.). The image is independent of ℓ.

We turn to hereafter the determination of the image of the ℓ-adic representation. Recall we have denoted the images of ρ_ℓ and ρ_λ by G_ℓ and G_λ, resp., and their Lie algebras in $gl(2,\mathbb{Q}_\ell)$ by $\mathfrak{g}_\ell$ and $\mathfrak{g}_\lambda$.

9. The CM case.

Theorem 14. Let f be a newform having complex multiplication by an imaginary quadratic field F. Then $\mathfrak{g}_\ell = F \otimes \mathbb{Q}_\ell$.

Proof. Note by thm.13 such an f comes from a Grossencharacter hence in view of §7.1 we have $K = F$. Then the restriction of ρ_ℓ on $H = Gal(\bar{\mathbb{Q}}/F)$ commutes with F. Therefore we have the representation:

$$\rho_\ell : H \longrightarrow GL(2, F \otimes \mathbb{Q}_\ell)$$

It is Abelian (thm.11). This system of ℓ-adic representations are locally algebraic by the theorem of Serre and Lang. Hence it comes from a representation of a Serre's torus associated to F with some module m (cf. the proof of thm.13; see also Part I):

$$r: S_m \longrightarrow GL(2, F \otimes \mathbb{Q}_\ell)$$

This representation is in fact defined over F. The facts that the image is Abelian and semi-simple together force that r has to be the map $S_m \longrightarrow F^\times \subseteq GL(2,F)$ (S_m associated to F!).

10. Forms without complex multiplication.

From now on, we will assume $k > 1$ and f does not have CM.

10.1. The case without extra twists.

Recall our representation

$$\rho_\ell: G \longrightarrow GL(2, K_\ell)$$

attached to a modular form f satisfying $\det \rho_\ell = \varepsilon \chi_\ell^{k-1}$, so on the open subgroup $H = \ker \varepsilon$ of G, $\det \rho_\ell(H) \subseteq \mathbb{Z}_\ell^{k+1}$. Therefore

$$\mathcal{G}_\ell \subseteq \mathcal{O}_\ell \triangleq \{ u \in gl(2, K_\ell) : \operatorname{tr}(u) \in \mathbb{Q}_\ell \}.$$

The equality does not always hold (though it seems to be) because there are extra operators on V_ℓ which commute with

G hence give more resriction.

10.1.1 The most apparent one may be (3) of §1.3.2. If $H = \ker \xi$ then

$$\mathrm{tr}\, \rho_\ell(H) \subseteq L \otimes \mathbb{Q}_\ell$$

and hence if k is even (which implies that the complex conjugate is in H, see §3.3) we have

$$\rho_\ell(H) \subseteq GL(2, L \otimes \mathbb{Q}_\ell) \subseteq GL(2, K \otimes \mathbb{Q}_\ell)$$

and

$$\mathcal{G}_\ell \subseteq \mathcal{G}_\ell = \mathcal{G} \otimes \mathbb{Q}_\ell \tag{4}$$

where $\mathcal{G} = \{ u \in gl(2,L) \mid \mathrm{tr}(u) \in \mathbb{Q} \}$

10.1.2 Next we assume k odd. Recall as mentioned in the Introduction V_ℓ is in fact a space of automorphic forms and now, there is an operator W on V_ℓ satisfying $W^2 = (-N)^{k-2}$ and

$$WaW^{-1} = \bar{a} \qquad \text{if } a \in K$$
$$W\rho_\ell(g) = \xi^{-1}(g)\rho_\ell(g)W = \rho_\ell(g)W\,\xi(g) \qquad \text{if } g \in G$$

(cf. §10.4 below). Let A be the algebra generated by W over K. This is a quaternion L-algebra. H acts on V_ℓ A-linearly. (Assume $\xi \neq 1$ hence $L \neq K$.) Now V is identified with the regular representation of A and $B = \mathrm{End}_A V \approx$

A (all over L). We see thus

Proposition 15. (Ribet [3] thm.5.5) For each ℓ

$$\rho_\ell(H) \subseteq \mathrm{Aut}_{A_\ell}(V_\ell) = (B\otimes Q_\ell)^\times$$

and furthermore

$$\rho_\ell(H) \subseteq \{ a \in (B\otimes Q_\ell)^\times \mid \det_{L_\lambda}(u) \in \mathbb{Q}_\ell \}.$$

From this proposition we have in particular

(5) $$\mathcal{J}_\ell \subseteq \mathcal{O}_\ell \hat{=} \mathcal{O}\otimes\mathbb{Q}$$

where $\mathcal{O} = \{ u \in B \mid \mathrm{tr}(u) \in \mathbb{Q}_\ell \}$.

Remark. $B\otimes\bar{\mathbb{Q}}_\ell \approx \mathrm{gl}(2, L\otimes\bar{\mathbb{Q}}_\ell)$.

10.1.3 When the $\mathcal{O}$ are chosen for k even and odd respectively with the inclusions (4) and (5), we have

Theorem 16. (Ribet [3] thm.5.7) The equlity does not hold iff f admits extra twists (see §10.2 for the definition).

Proof. Assume

$$\rho_\ell : H \longrightarrow GL(2, L\otimes\bar{\mathbb{Q}}_\ell)$$

and $\mathcal{O}_\lambda\otimes\bar{\mathbb{Q}}_\ell \subseteq \mathrm{gl}(2, L\otimes\bar{\mathbb{Q}}_\ell)$. For each embedding $\sigma : K \longrightarrow \bar{\mathbb{Q}}_\ell$

let

$$\rho_\sigma : G \longrightarrow GL(2, K\otimes\overline{Q}_\lambda) \longrightarrow GL(2, \overline{Q}_\ell)$$

corresponding to the decomposition for $K\otimes\overline{Q}_\lambda$. Now the used idea of "two principal" applies. In fact we have met similar situation in §11.1, Part II. The conditions there are satisfied now. The proof of the theorem of §11.1 Part II shows $\sigma_\ell \neq \sigma_\ell$ iff for some embeddings $\sigma \neq \tau$, V_σ and V_τ become isomorphic as modules of an open subgroup of G. We have at this time a character

$$\phi : G \longrightarrow \overline{Q}_\ell^\times$$

such that $\rho_\tau \simeq \rho_\sigma\otimes\phi$ which means exactly that f admits extra twists (see the proof in Ribet [3]). qed.

10.2. Extra twists.

Say f admits extra twisting if f has CM, or there are $\tau \in Aut(\mathbb{C}), \tau|L \neq id$, and a character $\phi : G \longrightarrow \mathbb{C}^\times$ unramified outside N such that

$$a_p = \tau(a_p)\,\phi(p)$$

for a set of primes p of density 1 (hence for almost all p).

There are examples indicating that some f indeed

admits extra twistings. As is seen above, this is the reason that deters $C_{\mathfrak{g}_\ell}$ from being equal to our above constructed Lie algebra.

10.3. Twisting group.

To avoid this obstruction, it is better to consider all twists. Momose does this. He calls such a pair (τ,ϕ) (or (σ,χ), symbolically) a twist of f. Then the basic fact is (characters are Dirichlet characters):

Proposition 17. (Momose [1] lemma 1.5)

(a) Each twist is of the form $(\sigma,\lambda\varepsilon^i)$ with λ is of order 1 or 2;

(b) For any two twists $(\sigma,*)$ and $(\tau,*)$, $\sigma\tau = \tau\sigma$ on K.

Put T = the set of twists. T turns out to be an (Abelian Galois) group under

$$(\sigma,\lambda)(\tau,\mu) = (\sigma\tau,\chi^\tau\mu)$$

For a number field L with $\sum$ the set of primes put

$$F_L = \mathbb{Q}(a_v : v \notin \sum, v/N)$$

L_f = the field corresponding to $\bigcap_{(\chi,\chi)\in T} \ker\chi$ and, $F_f = F_{L_f}$.

Being so

Propositon 18. (Momose [1] prop.1.7)

(a) K/F_f is an Abelian extension and $T \longrightarrow Gal(K/F_f)$ via $(\sigma, *) \longmapsto \sigma$ is an isomorphism;

(b) $F_L \supseteq F_f$ for any number fields L.

10.4. Twisting operators.

Momose essentially defines for each twist (σ, χ) a twist operator η_χ on V_ℓ ($\mathbf{Q}$-linear, but may not be K-linear in general). These twist operators satisfy

(a) $\eta_\chi a = a \eta_\chi$ if $a \in K$;

(b) $\eta_\chi F(p) = \chi(p) F(p) \eta_\chi$ if $p \nmid N$;

Let $D = \sum K\eta_\chi$, E = the centralizer of D in $\mathrm{End}_{\mathbf{Q}} V_i$. When these are ready, we have

Proposition 19. (Momose [1] thm.3.1)

(a) D is a $\mathbf{Q}$-subspace of $\mathrm{End}_{\mathbf{Q}} V$ and is $F_f \otimes \mathbf{Q}$-central simple. Moreover $\{\eta_\chi\}$ is a basis of the left K-vector space D;

(b) E is a quaternion algebra over F_f.

10.5. The Lie algebra.

We can now consider the Lie algebra $\mathcal{G}_\ell$. Let

$$\mathcal{T} = \{ x \in E : \mathrm{Trd}(x) \in \mathbb{Q} \}$$

where Trd = the reduced trace of E/F_f. Then

Theorem 20. (Momose [1] thm.4.1) $\mathcal{G}_\ell = \mathcal{T}_\ell = \mathcal{T} \otimes \mathbb{Q}_\ell$. for all .

Proof. Consider $G_f = \mathrm{Gal}(\overline{\mathbb{Q}}/L_f)$. By the definition of L_f and (b) of §10.4 G_f commutes with D. Together with the fact mentioned in §10.1, we have $\mathcal{G}_\ell \subseteq \mathcal{T}_\ell$. Let as usual

$$\overline{E} = E \otimes \overline{\mathbb{Q}}_\ell \qquad \text{and} \qquad \overline{E} = \prod_{\Gamma} E_\sigma$$

where σ runs through $\{ \sigma : F \longrightarrow \overline{\mathbb{Q}} \}$, and $E_\sigma = E \otimes_{F \otimes \mathbb{Q}_\ell} \overline{\mathbb{Q}}$ $M_\ell(\overline{\mathbb{Q}}_\ell)$ where $\overline{\mathbb{Q}}_\ell$ is an $F_f \otimes \mathbb{Q}_\ell$-module via

$$F \otimes \overline{\mathbb{Q}}_\ell \xrightarrow{\sigma} \overline{\mathbb{Q}}_\ell .$$

Consider

$$\begin{array}{ccccc} : G_f & \longrightarrow & E_\sigma^\times & \longleftarrow & \overline{E}^\times \\ & \searrow & \uparrow & \nearrow & \\ & & \mathrm{Aut}_D V_\ell = & E_\ell^\times & \end{array}$$

where $E_\sigma^\times \approx GL(2, \overline{\mathbb{Q}}_\ell)_\sigma$ (see the definition of E_σ). Let

$$\mathcal{G}_\sigma = \mathrm{Lie}(\mathrm{im}\, \rho_{\sigma, L_f}), \qquad \mathcal{T}_\sigma = \mathfrak{gl}(2, \overline{\mathbb{Q}}_\ell)_\sigma$$

We begin our argument, showing $\overline{\mathcal{G}_\ell} = \overline{\mathcal{H}_\ell}$, cf. the same method in Part II, §11.2.

Step (a). $\mathcal{G}_\sigma = \mathcal{H}_\sigma$, for each σ.

This follows from the irreducible thm.7 under the assumption the f does not have CM and the fact that $\det\rho_{\sigma,\iota_\ell}(G_f)$ is open in $\mathbb{Z}_\ell^\times$. In fact from semi-simplicity and thm.7 we have had $\mathcal{G}_\sigma \supseteq sl(2,\mathcal{O}_\ell)$.

Step (b). The map $\overline{\mathcal{G}_\ell} \longrightarrow \{(x, y) \in \mathcal{G}_\sigma \times \mathcal{G}_\tau \mid tr(x) = tr(y)\}$ is surjective for $\sigma \neq \tau$.

Otherwise, $V_\sigma \simeq V_\tau$ with $\sigma \neq \tau$ on F_f as $\mathcal{G}_\ell$-modules which is a fact seen before; or, considered as isomorphic modules of some open subgroup of G. So for some ϕ (see the proof of thm.16), $f^\sigma \simeq f^\tau \otimes \phi$. If one writes σ for $\sigma\tau^{-1}$ and ϕ for $\phi^{\tau^{-1}}$, he has

$f^\sigma = f \otimes \phi$ for some $\sigma \neq id$ on F_f.

But then $(\sigma, \phi) \in T$, and $\sigma \in Gal(K/F_f)$. This is a contradiction.

Step (c). The remaining is standard. qed.

11. The image of ρ_ℓ.

We shall discuss the image of the representation in

group level in this section. We follow Ribet [4]. Let $I(v)$ be an inertia subgroup of a place v of $\bar{\mathbb{Q}}$ over p.

Main lemma (Ribet [4] corol.1.2) There exists an open subgroup U of $I(v)$ such that $\rho_\lambda(g)$ is nilpotent for all $g \in U$ and $\lambda \nmid p$.

For $\rho_\lambda : G = Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL(2,\mathcal{O}_\ell)$ we let "$\sim$" denote the mod λ reduction:

$$\tilde{\rho_\lambda} : G \longrightarrow GL(2,\mathbf{F}_\lambda).$$

Theorem 21. (Ribet [4] thm.2.1) Let $H \subseteq G$ be an open subgroup. Then for almost all λ, the following statements hold:

(a) The representation $\tilde{\rho_\lambda}|H$ is an irreducible 2-dimensional representation of H over $\mathbf{F}_\lambda$;

(b) The order of $H_\lambda^{\sim}$ is divisible by $\ell(\lambda)$.

Proof.

Step 1: Reduce to the case $G = H$.

Assume the theorem is true for G. Let $h = [G:H]$. By (a) and (b) (cf. thm.23A) $G_\lambda^{\sim}$ will contain $SL(2,\mathbb{F}_\ell)$. But each orbit in $P^1(\mathbf{F}_\lambda)$ with respect to the action of $G_\lambda^{\sim}$ has cardinality $> \ell$ as is seen from the action by $SL(2,\mathbb{F}_\ell)$. So if $\ell > h$, H is also irreducible. Hence (a). (b) is obvious.

Step 2: Let's now prove the theorem for $H = G$.

First, consider a λ at which $\rho_\lambda^{\sim}$ is reducible. Then its semi-simplification is given by

$$\varepsilon_1 \chi_\ell^{\sim n} \oplus \varepsilon_2 \chi_\ell^{\sim m}$$

where $\ell = \ell(\lambda)$ and ε_i (see §9.3, Part I) are Dirichlet characters unramified outside N, m and n are determined modulo ℓ and $m + n \equiv k-1 \pmod{\lambda}$. Now

$$(6) \qquad a_p \equiv \varepsilon_1(p)\chi_\ell(F(p))^n + \varepsilon_2(p)\chi_\ell(F(p))^m$$
$$\equiv \varepsilon_1(p)\, p^n + \varepsilon_2(p)\, p^m \pmod{\ell}$$

This is in fact the situation corresponding to (a) of §4.3; but we can not deduce (a)' because of the ε_i's. However we remark that according to the main lemma (together with the unramified property) we have an open subgroup U of G, indepedndent of λ, at which the ε_i are trivial. Then from mod ℓ theory we can deduce (cf. §4.3 of Swinnerton-Dyer [1]) that among the n and m one is 0 and the other is $k-1$ (as Ribet claims). We consider this U which corresponds to a finite extension L, say, of $\mathbb{Q}$. For the primes which split completely in L (6) still has the form

$$a_p \equiv 1 + p^{k-1} \pmod{\ell} \quad \text{for} \quad p \nmid N.$$

This lifts to

$$a_p = 1 + p^{k-1}$$

which contradicts the Petersson conjecture. This finishes (a).

For (b), if it fails for a λ (cf. thm.10.A) there are possibilities listed there (and we use the notation there). For (1) $G_\lambda^{\sim}$ is contained in a Cartan subgroup which must split because of §3.4. We refer to (a). (3) occurs only finitely many times for otherwise the functon

$$F(g) = (\mathrm{tr}(\rho_\lambda(g))^2/(\det \rho_\lambda(g))$$

lifts to $G \longrightarrow \mathbb{Z}_\ell^\times$. However the image can not be finite which contradicts the conditions in thm.10A.

Finally we consider (b). We can consider only those λ such that $G_\lambda^{\sim}$ is contained in the normalizer N of a Cartan subgroup C but not in C. The quadratic extension K_λ corresponding to

$$G_\lambda^{\sim} \longrightarrow N/C = \{\pm 1\}.$$

is unramified outside N. Hence there only finitely many K_λ. If (2) fails for infinitely many λ we can choose a K simulteneous for still infinitely many λ. If ϕ is the Dirichlet character of K we have

$$a_p \equiv \phi(p)a_p \pmod{\lambda} \qquad \text{for } p \nmid N$$

form the evry definiton. It lifts to $a_p = \phi(p)a_p$ which means f has complex multiplication, contradictary to our assumption. qed.

Let D, E and F_f be as in § 10.4. We have seen that if $H = Gal(\overline{\mathbb{Q}}/L)$ (L_f there) then H commutes with D when all are considered as operators on V_ℓ. Therefore we have a realization:

$$\rho_\ell : H \longrightarrow (E \otimes \mathbb{Q}_\ell)^\times .$$

Again $n \circ \rho_\ell = \chi_\ell^{k-1}$ if n is the reduced norm of D over (extended automatically to D_ℓ). As has been shown that H is open in

$$\{ x \in E_\ell^\times : n(x) \in \mathbb{Q}_\ell^\times \}.$$

For almost all ℓ we have $E \otimes \mathbb{Q}_\ell \approx M(2, F \otimes \mathbb{Q}_\ell)$. Let R be the ring of integers of F_f. So $\rho_\ell | H$ has values in $GL(2,R_\ell)$ for suitably chosen basis. In fact $\rho_\ell | H$ has image in A_ℓ where

$$A_\ell = \{ u \in GL(2,R_\ell) : \det(u) \in \mathbb{Z}_\ell^{\times k-1} \}.$$

Theorem 22. (Ribet [4] thm.3.1) For almost all ℓ, $H_\ell = A_\ell$.

Proof. The group-theoretic technique is that used in § 4.4. For each ℓ prime to v let $a_v = tr(\rho_\ell(F(v)))$ (independent

of ℓ) where $F(v)$ is the Frobenius for H at v. We show that there is a place v of F such that a_v^2 generates F over $\mathbb{Q}$.

To see this we first show that there is an a_v such that a_v^2 generates F_λ over $\mathbb{Q}_\ell$. In fact, the set

$$U = \{ x \in H_\ell : (tr(x))^2 \text{ generates } F_\lambda \text{ over } \mathbb{Q}_\ell \}$$

is open because it is also the set of the x's that the subalgebra generated by $(tr(x))^2$ is of dimension equal to that of F_λ. We use the trick used in §4.4 to consider those prime numbers which split completely in L where $H = Gal(\overline{\mathbb{Q}}/L)$. We see for these ℓ A_ℓ admits a sequence $u_n \longrightarrow 1$ having the property described in the definition of U. As H_ℓ is open in A_ℓ, we find $U \neq \phi$. Cebotarev's Density Theorem hereof implies the existence of a v. Such an a_v will turn out to fit almost all ℓ. But from the data in §3 that a_v is an algebraic number so $a_v \in R$. It follows that a_v^2 generates F over $\mathbb{Q}$ and consequently R_λ over $\mathbb{Z}$ for almost all ℓ.

With this fact (set $x = \rho_\lambda(F(v))$) and the previous theorem, we compare thm.20A & 22A. The map

$$H \longrightarrow GL(2, \mathbb{Z}_\ell) \longrightarrow \mathbb{Z}_\ell^{\times k-1}$$

which is χ_ℓ^{k-1}, is surjective for almost all ℓ (those prime to $[G:H]$). We are done.

Part IV Appendix: Group Theory

0. We will generally use p to denote a prime number in this chapter.

1. The group theory of $GL(2)$ plays an important role in the determination of the images of the Galois representations. In fact the dimension 2 is essential in most of the techniques we meet. We collect here some of the frequently used results for convenience.

2. Assume G is a subgroup of $\prod GL(2,\mathbb{Z}_p)$, G_p its projection to each factor $GL(2,\mathbb{Z}_p)$, $\tilde{G_p}$ is the "mod p" image of G_p in $GL(2,\mathbb{F}_p)$, i.e., modulo p entrywise.

The result from the openness of all G_p to the openness of G indicats the "independent of p, for almost all p".

Theorem 1. (Serre [6] IV §3.1 main lemma) Assume G is closed, and that

(1) G_p is open in $GL(2,\mathbb{Z}_p)$ for all p;

(2) The image of G by det: $\prod GL(2,\mathbb{Z}_p) \longrightarrow \prod \mathbb{Z}_p^{\times}$ is

open;

(3) $G_p^{\sim}$ contains $SL(2,\mathbb{F}_p)$ for almost all p.

Then G is open in $\prod GL(2,\mathbb{Z}_p)$.

Remark The theorem can be slightly generalized, see thm.16.

3.

Theorem 2. (Serre [6] IV §3.4 lemma 1) $PGL(2,\mathbb{F}_p)$ is simple if $p \geq 5$. Every proper subgroup of $PGL(2,\mathbb{F}_p)$ is solvable, or isomorphic to the alternative group A_5. The last possibility occurs only if $p \equiv \pm 1 \pmod 5$.

Theorem 3. (Serre [6] IV 3.4 lemma 2) No proper subgroup of $SL(2,\mathbb{F}_p)$ maps onto $PSL(2,\mathbb{F}_p)$.

The following theorem shows why we can use the method of mod p.

Theorem 4. (Serre [6] IV §3.4 lemma3) Let H be a closed subgroup of $SL(2,\mathbb{Z}_p)$ whose "mod p" image in $SL(2,\mathbb{F}_p)$ is the whole $SL(2,\mathbb{F}_p)$. Assume $p \geq 5$, then $H = SL(2,\mathbb{Z}_p)$.

4. We now consider subgroups of $GL(2)$ over finite fields. For a field $\mathbb{F}_q$ of $q = p^n$ elements we would write $GL(2,q)$ rather than $GL(2,\mathbb{F}_q)$. Similr for $gl(2,q)$ and $PGL(2,q)$ etc.

4.1 $\#GL(2,q) = (q-1)^2 q(q+1)$.

4.2 Cartan subgroups ($q = p$)

(a) Split: $C: \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$ type $(p-1, p-1)$.

Semi-split: $C': \left\{ \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix} \right\}$ cyclic of order $p-1$.

$C = C' \cdot \mathbb{F}_p^{\times}$. (In particular the only Cartan subgroup containing C' is C.) They have the same image in $PGL(2,p)$ cyclic of order $p-1$.

(b) Non-split. If $k \subseteq gl(2,p)$ is a field of p^2 elements, i.e. a quadratic extension of $\mathbb{F}_p$, then the non-split Cartan subgroup will be $k^{\times}$. It is cyclic of order p^2-1, with image in $PGL(2,p)$ cyclic of order $p+1$.

4.3 The intersection of all Cartan subgroups is $\mathbb{F}_p^{\times}$; and their union is the set of elements of order prime to p.

4.4 For $s \in GL(2,p)$ such that $Tr(s)^2 - 4\det(s) \neq 0$, (cf. end of thm 16.) it is contained in a unique Cartan subgroup. This Cartan subgroup splits if $Tr(s)^2 - 4\det(s)$ is quadratic residue. Note every non-center element of a non-split Cartan subgroup has no fixed line.

4.5 Assume that C is a Cartan subgroup, N its normalizer. ($p \neq 2$ if C splits.)

(a) C splits then $N = C \cup \left\{\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}\right\}$, $[N:C] = 2$. If $s \in N \setminus C$ Then $Tr(s) = 0$.

(b) C is non-split then, if $s \in N \setminus C$, $x \longmapsto sxs^{-1}$ is the Frobenius! So $sas^{-1} = a^p$ for any a in C. Again $[N:C] = 2$ and $s \in N \setminus C$ implies $Tr(s) = 0$.

(c) Let $\overline{C}$, $\overline{N}$ be the images of C and N in PGL, respectively. Then $\overline{N}$ is the normalizer of $\overline{C}$, which is a diedral group.

4.6 Borel subgroups

$$B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}, \quad \text{order } p(p-1)^2.$$

Obviously a Cartan subgroup contained in a Borel subgroup must split.

Theorem 5. (Serre [8] §2.2 prop.14) Let C be a Cartan subgroup in GL(2,p) and N its normalizer. Assume C' is a Cartan subgroup (resp. semi-split-Cartan subgroup) contained in N. Suppose $p \geqslant 5$ if C' split, $p \geqslant 3$ otherwise. We have $C' = C$ (resp. $C' \subsetneq C$).

5. We continue §4. G is a subgroup of GL(2,p) in the sequal.

Theorem 6. (Serre [8] §2.5 prop.15) If G is of order divisable by p, then G contains SL(2,p), or is contained in a Borel subgroup.

In the following theorems 7-9 k is any field.

Theorem 7. (Serre [8] §2.5 prop.16) Suppose H is a finite subgroup of $PGL(2,k)$ of order prime to the characteristic of k. Assume H is neither cyclic nor dihedral, then H is isomorphic to A_4, S_4, or A_5. In particular H is of order 12, 24, 60, its elements are of order 1, 2, 3, 4 and 5.

Theorem 8. (Serre [8] §2.5 corol.) If $\mathrm{chark} = 2$ or 3, all finite subgroups of $PGL(2,k)$ of orders prime to char.k are cyclic or dihedral.

Theorem 9. (Serre [8] 2.5 Remarque) $PGL(2,k)$ contains

(1) A_4 iff, $\exists\, x \in k$ such that $x^2+x = 1$ if char.k=2, $\exists\, y, z \in k$ such that $y^2+z^2 = -1$ if char.k $\neq 2$.

(2) S_4 iff char.k $\neq 2$ and $\exists\, y, z \in k$ such that $y^2+z^2 = -1$.

(3) A_5 iff $\exists\, x, y, z \in k$ such that $x^2+x = 1$ and $y^2+z^2 = -1$.

Theorem 10. (Serre [8] §2.6) Let G be of order prime to p, H its image in $PGL(2,p)$. Then we have the following cases:

(1) H is cyclic, contained in a Cartan subgroup of PGL unique if $H \neq 1$. We conclude that G is contained in a Cartan subgroup.

(2) H is dihedral, containing a cyclic subgroup C', nontrivial of index 2. C' is contained in a unique

Cartan subgroup C of PGL, H is the normalizer of C. We conclude that G is contained in the normalizer of a Cartan subgroup.

(3) H is isomorphic to A_4, S_4, A_5, and the final case occurs only if $p \equiv \pm 1 \pmod 5$. We see that if $s \in G$ then $u = Tr(s)^2/det(s)$ is equal to 4, 0, 1, 2 or satisfies $u^2 - 3u + 1 = 0$.

Theorem 11. (Serre [8] §2.7 prop.17) Assume that G contains a Cartan subgroup C (resp. semi-split-Cartan subgroup), and $p \neq 5$ if C splits. Then one of the following holds:

(1) $G = GL(2,p)$;

(2) G is contained in a Borel subgroup;

(3) G is contained in the normalizer of a Cartan subgroup.

Theorem 12. (Serre [8] § 2.8 prop.18) Assume that G contains a Cartan subgroup C (resp. semi-split-Cartan subgroup). Suppose $p \neq 2$ and G is normal, then $G = GL(2,p)$.

Note that $Tr(s)^2-4det(s)$ is the square of the difference of the eigenvalues of $s \in GL(2)$.

Theorem 13. (Serre [8] §2.8 prop.19) Suppose $p \geq 5$ and the following conditions hold:

(1) $\exists\, s \in G$ such that $Tr(s)^2-4det(s)$ is a non-zero quadratic residue in $\mathbb{F}_p$ and $Tr(s) \neq 0$;

(2) $\exists\, s' \in G$ such that $Tr(s')^2-4det(s')$ is a quadratic

non-residue in $\mathbb{F}_p$ and $Tr(s') \neq 0$;

(3) $\exists\, s'' \in G$ such that $u = Tr(s'')^2/\det(s'')$ is distinct from 0, 1, 2, 4, and $u^2-3u+1 \neq 0$.

Then G contains $SL(2,p)$. In particular if $\det: G \longrightarrow \mathbb{F}_p^\times$ is surjective then $G = GL(2,p)$.

Theorem 14. (Serre [8] §2.8 corol.) Assume the following hypothesis holds:

(*) For any $t \in \mathbb{F}_p$ and any $d \in \mathbb{F}_p^\times$ there is an s in G such that

$Tr(s) = t$ and $\det(s) = d$.

Then $G = GL(2,p)$.

6. The following results are related to the case of the product of finitely many representations. Assume k is a positive even integer. K is a field. A subgroup G of $GL(2,K)$ is semi-simple if it acts on $K \oplus K$ semi-simply.

Theorem 15. (Ribet [1] §2 thm.2.1) Assume that $K_1, K_2, \cdots, K_t$ are finite extensions of $\mathbb{Q}_p$ ($p \geq 5$), $O_1, O_2, \cdots, O_t$ the rings of the integers. Let G be a closed subgroup of

$$GL(2,O_1)\times\cdots\times GL(2,O_t)$$

whose "mod p" image in

$$GL(2,O_1/pO_1)\times\cdots\times GL(2,O_1/pO_2)$$

contains

$$SL(2,O_1/pO_1)\times\cdots\times SL(2,O_t/pO_t).$$

Then G contains

$$SL(2,O_1)\times\cdots\times Sl(2,O_t).$$

Theorem 16. (Ribet [1] §2 corol.2.2) Suppose G is a closed subgroup of

$$A = \left\{ (u_1, \cdots, u_t) \in \prod GL(2, \mathcal{O}_i) : \det u_1 = \cdots = \det u_t \right\}$$

which satisfies:

(1) $\det(G) = \mathbb{Z}_p^{\times k-1}$;

(2) The image of G "mod p" in $\prod GL(2, \mathcal{O}_i/p\mathcal{O}_i)$ contains $\prod SL(2, \mathcal{O}_i/p\mathcal{O}_i)$;

Then $G = A$.

Theorem 17. (Ribet [1] 2 thm.2.3) Let G be a compact semi-simple subgroup of $GL(2,K)$, where K is a finite extension of $\mathbb{Q}_p$. Suppose that G has an open Abelian subgroup N, but $[G : G \cap K^\times] = \infty$. Then G has an open Abelian subgroup of index 1 or 2.

Let $M = \mathbb{F}_{q_1}^\times \times \cdots \times \mathbb{F}_{q_t}$; it is an $\mathbb{F}_p$-algebra.

Theorem 18. (Ribet [1] § 3 thm.3.1) Let G be a subgroup of

$$A = \left\{ (u_1, \cdots, u_t) \in \prod GL(2, q_i) : \det(u_1, \cdots, u_t) \in \mathbb{F}_p^{\times k-1} \right\}$$

which satisfies

(1) $\det: G \longrightarrow \mathbb{F}_p^\times$ is surjective;

(2) G contains an element x such that $(\mathrm{Tr}(x))^2$ generates the $\mathbb{F}_p$-algebra M;

(3) The image of each projection $r_i: G \longrightarrow GL(2, q_i)$ is an irreducible subgroup of $GL(2, q_i)$ whose order is divisible by p.

Then $G = A$.

Let A be a subgroup of $B \times B'$ for which the projections $r: A \longrightarrow B$, $r': A \longrightarrow B'$ are surjective, with kernels N, N', respectively.

Theorem 19. (Ribet [1] §3 lemma 3.3) The image of A in $B/N \times B'/N'$ is the graph of an isomorphism

$$B/N \longrightarrow B'/N'.$$

Theorem 20. (Ribet [1] § 3 lemma 3.4) Let $S_1, \cdots, S_t$ ($t > 1$) be finite groups with no non-trivial Abelian quotients. Let G be a subgroup of

$$S = S_1 \times \cdots \times S_t$$

such that each projection

$$G \longrightarrow S_i \times S_j \qquad i \neq j$$

is surjective. Then $G = S$.

Theorem 21. (Ribet [1] § 3 lemma 3.4) Let $T_1, \cdots\cdots, T_t$ ($t > 1$) be profinite groups. Assume for each i that the following condition is satisfied: for each open subgroup U of T_i, the closure of the commutator subgroup of U is open in T_i. Let G be a closed subgroup of

$$T = T_1 \times \cdots \times T_t$$

which maps onto an open subgroup to each $T_i \times T_j$. Then G is open in T.

Assume A is subgroup of $GL(2,q) \times GL(2,q')$ containing a (u, u') such that $\det(u) = v^k$ and $\det(u') = v^{k'}$ for some pair of even integers (k, k') and a v. G is a subgroup of A. The following theorem helps us to apply the "two principle".

Theorem 22. (Ribet [1] §3 thm.3.8) Assume A and G has the same projections B and B' to GL(2,q), GL(2,q'). Suppose $G \subsetneq A$ but $G \neq A$. Then $q = q'$ and, there is a $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and a character $\xi : G \longrightarrow \mathbb{F}_q^{\times}$ such that, for any (u, u') in G:

$$\mathrm{tr}(u') = \xi(u, u')\, \mathrm{tr}(u)^{\sigma},$$

$$\det(u') = (\xi(u, u'))^2 \det(u).$$

Theorem 23. (Ribet [1] § 3 thm.3.6) Let $p \geq 5$, $q = p^n$. Suppose that G is a subgroup of PSL(2,q) whose order is divsible by p and is "irreducible" in the sense that it acts without fixed points on $P^1(\mathbb{F}_q)$. Then there is a subfield K of $\mathbb{F}_q$ such that G is conjugate either to PGL(2,K) or PSL(2,K).

7. Similar results hold for subalgebras in gl(2), and simpler.

7.1 Let V be a 2-dimensioal vector space, X be a line in V. We have the following subalgebras of gl(V):

(a) Borel subalgebra $b_X = \{ u \in gl(V) : u(X) \subseteq X \}$;

(b) $r_X = \{ u \in gl(V) : u(V) \subseteq X \}$;

(c) $n_X = \{ u \in gl(V) : u(V) \subseteq X \ \& \ u(X) = 0 \}$.

They can be represented by the matrices of the following forms, respectively:

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \qquad \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}$$

under suitably chosen basis.

7.1.1 Cartan algebra.

It is a subalgebra of dimension 2 which acts semi-simply on V.

7.1.1.1 Split Cartan subalgebra: it can be represented by the matrices of the following form:

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

7.1.1.2 Non-split Cartan subalgebra: it is a quadratic field extension of the definition field.

7.2

Theorem 24. (Serre [2] §1.4 prop.2) A Lie subalgebra of $gl(V)$ properly containing a Cartan subalgebra C is either a Borel subalgebra or $gl(V)$. The former case is impossible if C is non-split.

7.3

Theorem 25. Assume that $\mathfrak{S}_1, \cdots, \mathfrak{S}_n$ are simple finite dimensional Lie algebras and U is a subalgebra of $\prod \mathfrak{S}_i$. If for any $i < j$ the projection $U \longrightarrow \mathfrak{S}_i \times \mathfrak{S}_j$ is surjective, then

$U = \prod S_i$.

Theorem 26. Under the same assumption of the preceeding theorem, if J is an ideal of $\prod S_i$, then J is a diredt product of the S_i's.

REFERENCES

Apostal, T.M.,

[1] Introduction to Analytic Number Theory, Springeer-Verlag, 1976

Carayol, H.,

[1] Sur la Mauvaise Reduction des Courbes de Shimura, C. R. Acad. Sc. Paris 296, 557-560 (1983).

[2] Sur les Representations ℓ-adiques attachees aux Formes Modulaires de Hilbert, C. R. Acad. Sc. Paris 296, 629-632, (1983).

Cassels, J.W.S. & Frohlich, A.,

[1] Algebraic Number Theory, Thompsen Book comp. Inc. Washington D.C., 1967

Deligne, P.,

[1] Forms Modulairs et representations ℓ-adiques, Seminair Bourbaki 355, Fevrier, 1969, Lecture Notes in Math. 179, Berlin-Heidelberg-New York, Springer, 1971.

[2] Forms Modulairs et Representations de GL(2), Lecture Notes in Math. 349, 55-105, (1973).

Deligne, P., Serre, J.-P.,

[1] Forms Modulairs de Poids 1, Ann. Scient. Ec. Norm. Sup. 4 serie 7, 507-530 (1974).

Fontaine, J.-M.,

[1] Representations p-adiques, proceed. ICM 1983, Warszwa

Frohlich, A.,

[1] Formal Groups, Lecture Notes in Math. 74, Spinger-Verlag, 1968

Gross, B.H.,

[1] Arithmetic on Elliptic Curves with Complex Multiplication, Lecture Notes in Math. 776,

Hardy & Wright

[1] An Introduction to the Theory of Numbers, 5th Edition, Oxford University Press, 1979

Harvey,

[1] Discrete Groups and Automorphic Functions, Acad. Press, 1977

Katz, N.,

[1] p-adic Properties of Modular Schemes and Modular Forms, International Summer School on Modular Functions: Antwerp, Lecture Notes in Math., 350, 69-190, 1973.

[2] A Results on Modular Forms in Characteristic p, Lecture Notes in Math. 601, 53-61, 1977.

Lang, S.,

[1] Elliptic Functions, Addison-Wesley Publ. Comp. Inc. 1973

Momose, F.,

[1] On the ℓ-adic Representations attached to Modular Forms, J. Fac. Sci. Univ. Tokyo, 28 (1981) 89-107.

Mumford, D.,

[1] Abelian Varieties, Oxford University Press, 1974

Rankin, R. A.,

[1] Contributions to the Theory of Ramanujan's Function $\tau(n)$ and Similar Arithmetic Functions, Prop. Cambridge Phil. Soc., 35 (1939) I & II, p.351-372

Ribet, K.A.,

[1] On ℓ-adic Representations attached to Modular Forms, Inventiones Math., 28 (1975), 245-275.

[2] Galois Action on Division Points of Abelian Varieties with Real Multiplications, Am. J. Math., 98 (1976), 751-804.

[3] Galois Represntations attached to Eigenforms with Nebentypus, Lecture Notes in Math., 601, 17-52, (1977).

[4] On ℓ-adic Representations attached to Modular Forms II, preprint.

Robert, A.,

[1] Elliptic Curves, Lecture Notes in Math., 326,

Serre, J-P.,

[1] Sur les Groupes de Congrunce des Varietes Abeliennes, Izv. Akad. Nauk. SSSR, 28, 1964, 3-20.

[2] Groupes de Lie ℓ-adiques attaches aux courbes elliptiques, Colloque Clermont-Ferrand, 239-256,

C.N.R.S. 1964.

[3] Lie Algebra and Lie Groups, Benjamin, New York, 1965.

[4] Une Interpretation des congruences relatives a la fonction de Ramanujan, Seminair Delange-Pisot-Poitou, 1967-1968, ex. 14.

[5] Corps Locaux, (2eme edition) Paris, Hermann 1968.

[6] Abelian ℓ-adic Representations and Elliptic Curves, Benjamin, New York, 1968.

[7] Congruences et Forms Modulaires (d'apres H.E.P. Swinnerton-Dyer), Seminair Bourbaki, 416, Juin, 1972, Lecture Notes in Mathematics, 317, Springer, Berlin-Heidelberg-New York, 1973.

[8] Proprietes Galoisiennes des Points d'Ordre Fini des Courbes Elliptiques, Inventiones Math., 15 (1972), 259-331.

[9] Lectures on Modular Forms of Weight 1, Proceedings of the 1975 Durham Conference on Number Theory.

[10] Sur les groupes de Galois attaches aux groupes p-divisibles, Prceed. Conf. on Local Fields, Springer-Verlag, Berlin, 1967.

[11] Representations ℓ-adiques, Symmposiam on Algebraic Number Theory, Kyoto 1976, S.Iyanaga (Ed.) Japan Soc. for the Promotion of Scie., Tokyo, 1977

Serre, J.-P., Tate, J.,

[1] Good Reduction of Abelian Varieties, Ann. of Math. 88, 492-517 (1968)

Shimura, G.,

[1] Introduction to the Arithmetic Theory of Automorphic

Functions, Publ. Math. Soc. Japan, No.11, Tokyo-Princeton, 1971.

[2] Algebraic Number Fields & Sympletic Discontinuous Groups, Annals of Math, 86, (1967), pp 503-592.

Shimura, G., & Taniyama, Y.,

[1] Complex Multiplication of Abelian Varieties and its Applications to Number Theory, Math. Soc. Japan, Tokyo, 1961

Swinnerton-Dyer, H.P.F.,

[1] On ℓ-adic Rpresentations and Congruences for Coefficients of Modular Forms, International Summer School on Modular Functions, Antwerp, 1972, Lecture Notes in Mathematics, 350, Springer, Berlin-Heidelberg-New York, 1973.

Tate, J.,

[1] p-divisible Groups, Proc. Conf. on Local Fields, Spinger-Verlag, Berlin, 1967.

[2] The Arithemetic of Elliptic Curves, Inv. Math., 23, 179-206, (1974)

[3] Algebraic Cycles and Poles of Zeta Functions, in "Arithmetic Algebraic Geomettry", Harper and Row, New York, 1965

Weil, A.,

[1] On Certain Type of Characters of the idele-class Group of an Algebraic Number Field, Proc. Inter. Symp. Tokyo-Nikko, 1955, 1-7.

[2] Basic Number Theory, Berlin-Heidelberg-New York, Spinger

1967.

[3] Adeles and Algebraic Groups, Princeton, IAS, 1961

[4] Courbes Algebriques et Varietes Abeliennes, Hermann, 1971